

**R20.109 ISO 28000:2007 Supply Chain Security**

**Management Systems Supplement**

|  |
| --- |
|  |

1.0 **Scope** - This R20.109 applies to organizations requiring assessment and/or registration of their supply chain security management system in accordance with ISO 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 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 Supply Chain Security Management System Audit and Certification implementations (SCSMS) for auditing against ISO 28000:2007 and 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 17021-1, ISO 28000:2007, 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 28000:2007 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 Supply Chain Security 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 Supply Chain 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 SCSMS implementation and audit.

1. **Purpose** - The purpose of this document is to outline the process for providing organizations and their suppliers with assessment and registration of their Supply Chain Security Management System. It provides requirements for auditing organizations to ISO 28003:2007 and normative documented information and aligns with current ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 guidance.
2. **References**

* EA-7/03 – February 2000 – EA Guidelines for Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems.
* ISO 28003:2007 – Security Management Systems for the Supply Chain – Requirements for bodies providing audit and certification of supply chain security management systems.
* ISO 28000:2007 – Specification for security management systems for the supply chain.
* ISO 28001:2007 – Security management systems for the supply chain- Best practices for implementing supply chain security, assessments, and plans – Requirements and Guidance
* ISO/IEC 17021-1:2015 – Conformity assessment – Requirements for bodies providing audit and certification of management systems.

2.0 **Definitions**

2.1 Certified Client: organization whose supply chain security management system has been certified/registered by a qualified third-party.

2.2 Impartiality: actual and perceived presence of objectivity.

2.3 Management system consultancy and/or associated risk assessments: participation in designing, implementing, or maintaining a supply chain security management system and in conducting risk assessments.

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 17021-1:2015. 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 27001:2013 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.

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 SCSMS 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 28000:2007 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-ASQ 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 28000:2007 and submitted same for review and consideration/approval by ANAB. Supply Chain Security sector qualification consists of an application review, witness audit, and recommendation for the recognition of SRI’s Supply Chain Security Management System program.

4.2 SRI has prepared an application form for the applicable Supply Chain Security Management System (SCSMS) registration. This application provided the ANAB with confidence that SRI has developed the necessary documented process to meet ISO 28000:2007 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 28000:2007-based witness audit per year.

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

4.5 SRI does not offer consulting services or internal audits to clients of registration services.

4.6 SRI has a security clearance process for candidate security auditors as well as other personnel. It is facilitated by the HR department. Criminal background checks are conducted, and SRI verifies legally required evidence of US citizenship or other accepted documentation authorizing individuals to work in the US. If the auditors have other security clearances, those records are collected for their file. Candidates go through an interview process with the Associate V.P., Certification as well as other key managers to understand not only competence, but trustworthiness and appropriate communication skills / behavioral characteristics. Work history for candidates is provided via resume and confirmed and must contain at least five (5) full continuous years.

4.7 Upon hire and full qualification as a Security Auditor, SRI will provide tamper proof ID cards including photograph, name, SRI’s name and logo.

4.8 Upon request by organizations undergoing audit, SRI will provide auditor confidentiality documentation.

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. Additional requirements in excess of ISO/IEC 17021 require mention of relevant standard(s) and/or other normative documentation. As mentioned previously, ISO/IEC 17021-1, ISO 28000, and ISO 28001 may be referenced here (depending on scope and criteria requirements of the specific organization under audit).

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 28000:2007.

1. The essential elements of competence required to perform SCSMS 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.
   1. SRI’s processes and requirements to obtain ISO 28000:2007 sector qualification include as a minimum:
2. Evidence that the SRI has individuals with appropriate background, experience, and knowledge. (Contract Review will have Oversight by that individual.) Knowledge and competence are gained by attending and passing an ISO 28000:2007 Transition Auditor course. Items listed under “B” below are also added competencies gained by attending the ISO 28000:2007 course. Appropriate background and experience are a plus.
3. Evidence of SRI’s criteria for the training and selection of audit team ensures appropriate levels of:
   * + A basic knowledge of the requirements of ISO 28000:2007(E) and related standards in the series
     + A basic knowledge of Security in Supply Chain Management Systems
     + Understanding of the processes necessary to design, document, and implement a Supply Chain Security Management System (SCSMS) conforming to the requirements of ISO 28000:2007
     + Basic knowledge of International and Country-specific Legal and Regulatory requirements for the Supply Chain
     + Understanding of concepts, tools, and methodologies for assessing and managing Supply Chain Security
     + Understanding of Supply Chain Security audit criteria
     + Understanding of Supply Chain incident Management
     + Understanding of the documented information and evidence necessary to display conformity to ISO 28000:2007

This training is gained by attending and passing an approved ISO 28000:2007 Transition Auditor training course. Records of test completion and satisfactory course completion are maintained in SRI auditor/contractor files.

1. Documented auditor training program reviewed and approved by the ANAB prior to or during the qualification process that conforms to ISO 28000:2007 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 28000:2007 standard
   2. Generally accepted course content, format, and training objectives
   3. The scheme as used in the specific sector for Certification/Registration of ISO 28000:2007.
2. 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;
3. A University Degree (extensive experience and supplementary professional education and training can be equivalent);
4. 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;
5. Proof of attending and passing a 3-day SCSMS transition auditor course;
6. 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;
7. Qualification to ISO/IEC 27001:2013 ISMS through Exemplar Global (formerly RABQSA) and/or IRCA is preferred and the auditor exhibits the following attributes: objectivity, maturing, discerning nature, analytical, persistent, and realistic. Understands complex operations and able to understand the role of individual units in a larger organization;
8. 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;
9. All relevant experience should be reasonably current;
10. Keep up own knowledge and skill in information security and auditing.
11. SRI has specific procedures, tools, and techniques in its system for granting, maintaining, extending, reducing suspending, and withdrawing certification/registration.
12. A full system witness audit from a recognized AB such as ANAB of an SCSMS audit.
13. SRI agrees to periodic surveillance and witness audits by ANAB.
14. No Certificates or approvals to ISO 28000:2007 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.
15. 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).
16. SRI requires the applicant to prepare a Statement of Application, Security Plan, and Security Declaration describing which parts of the SCSMS standard or normative document are relevant and applicable for the organization’s SCSMS. The Statement of Application 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.
17. SRI will ensure that the organization’s supply chain security scope, security declaration, and risk assessment properly reflect its activities and the boundaries of its supply chain applicability as defined in the SCSMS standard, AEO (authorized economic operator) certification(s), and/or normative documentation. SRI 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 SCSMS shall be addressed as needed subject to applicable criteria and shall be included in the analysis of the organization's supply chain security risk assessment.
18. 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 28000:2007 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 28000:2007 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 **Requirements for Auditors**

* 1. SCSMS auditors shall, as a minimum, continually meet the education, training, work experience and audit experience of ISO 19011, ISO 28000:2007, and ISO 28003:2007 and satisfy the following criteria:

1. Auditing Experience - To have participated in at least four audits for a minimum of 20 days, that cover all the elements of the ISO 28000:2007 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 SCSMS 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 28003:2007;
   4. the principles and processes related to supply chain risk assessment and risk management;
   5. principles relating to supply chain security planning, documented information, control selection, and implementation. and
   6. general management system and specific supply chain security management system auditing principles.
2. The auditor must be trained in SCSMS requirements. This training covers all those noted in A. above and as specified in ISO 28003:2007 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.
3. The following requirements apply to the audit team as a whole:
4. 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:
   1. managing the team,
   2. knowledge of the legislative and regulatory requirements and of legal compliance in the particular supply chain security and industry-specific AEO field(s),
   3. identifying supply chain security threats,
   4. identifying the supply chain vulnerabilities of the organization and business partners within the statement of application/supply chain scope, and understanding their impacts, mitigation of risks, and selection of appropriate controls,
   5. knowledge of current criteria, requirements, and technical and administrative guidance and requirements pertaining to applicable supply chain sectors and AEO’s,
   6. knowledge of risk assessment related to supply chain security.
5. The audit team should be competent to trace indications of security incidents in the organization's SCSMS back to the appropriate elements and components of the supply chain.
6. An audit team may consist of one person provided that the person meets all the criteria set out in A. above.
   1. To maintain SCSMS auditor qualification, all auditors must participate in at least five ISMS / SCSMS audits per calendar year or carry out a minimum of 10 on-site audit days per year. Other Information security audits, such as CMMC or ISO 27701 can also be used to demonstrate minimum activity. 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 as described in 6.3.
   2. SRI will produce an annual continual training plan appropriate for each SCSMS auditor. Progress toward fulfilling the plan will be assessed at each annual auditor review. The training will address security methodologies, risk analysis and management principles, analysis of critical control point, audit techniques and competence items mentioned un 7.2.3.1 of ISO 28003:2007. Training will:
      1. be planned based on the analysis of needs on the subjects and competence given above.
      2. be recorded
      3. include audit case studies allowing an auditor’s competence to be evaluated.
      4. be supported by interpretations of the SCSMS standard, FAQS, workshop records and standard corrections on the case studies.
      5. be evaluated with proper actions on the basis of training / testing results.
      6. be performed by qualified trainers.

7.0 **Requirements for Assessment and Reporting**

7.1 **SCSMS Assessment Teams**

1. The assessment team leader must be a qualified SCSMS lead auditor per applicable Authority guidance and as identified in SRI’s accredited system. When different teams are used to audit multiple sites, the Lead Auditor will coordinate all audit teams and manage the development of a synthesis report (i.e., single report of all locations).
2. The team may include other auditors that are approved per SRI.
3. The assessment team shall include an auditor qualified for the organizational and supply chain commodities (i.e., AEO Certification, Industry, Statement of Application, and Declaration Categories). 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. SCSMS credentials are the minimum.
4. 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 28000:2007 as may affect the scope and application of the assessment activity. The SCSMS Lead Auditor shall provide guidance to the assessment team throughout the assessment on the interpretation of requirements and, when requested, the significance of any issues identified. Important deviations from common elements of Scope for other standards, which key management and audit personnel must be aware, include the following;

* There is a “unique need for confidentiality..” when auditing and certifying an organization to Supply Chain Security Management System criteria. This stems from information discovered during the risk assessment, planning, implementation, corrective/preventive action, and emergency response processes that may be of particular risk in terms of unauthorized access. Confidentiality aspects are mentioned frequently in different clauses of ISO 28003:2007 (covering Background Investigations, Security Clearance, Information/Data Security, Secure Transmission, etc). In summary, Confidentiality requirements demand assurance regarding the personal integrity of auditors and CB management (including criminal background investigations, clearance adjudications, checking of credit history, etc.), protection of information throughout the supply chain, and secure communication and transmission of SCSMS data and information. It is unique in that no other Management System standard imposes these requirements (see following appropriate clause interpretations for additional guidance).
* There is brief mention of “..other sets of specified supply chain security management system requirements..” which may be applicable to an SCSMS implementation. It is important for CB personnel to know that ISO 28000:2007 is the First-Tier, basic Requirements Specification for SCSMS. In addition, ISO 28001:2007 may commonly be selected or imposed as a Second-Tier Requirements Specification for extension of basic SCSMS implementations (for example, if WCO SAFE Framework requirements are imposed on an organization). It is the organization’s responsibility to identify whether supplemental SCSMS requirements are relevant; it is the Auditor’s responsibility to ensure that the organization has done due diligence in selecting all relevant Requirements Specifications and appropriate mandatory Legal, Regulatory, Industry, Governmental, and Intergovernmental requirements and criteria to satisfy SCSMS intent and the protection of the supply chain as appropriate to the scope of the SCSMS.

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. The certification body shall have access to the necessary technical expertise for advice on matters directly relating to certification for technical areas, types of supply chain security elements and geographic areas in which the certification body operates. Such advice may be provided externally or by certification body personnel.

7.2 **Duration of Assessment**

* + 1. An estimation of time 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, 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 28003:2007, Annex A, Table A.1, and Annex B (Multiple Sites) to determine auditor time. Guidance for calculating mandays is as follows;

* The starting point for mandays will be based on the number of effective employees in Table A.1.
* All attributes of the organization’s facility, site, systems, processes, and products/services should be considered and a fair adjustment can be made based on the justifiable factors in Table A.1. Additive factors may be off-set by subtractive factors. In all cases where adjustments are made to the time provided in the Auditor Timetable, sufficient evidence and records shall be maintained to justify the variation.
* A site plan should be obtained especially for large site and organizations to help with evaluating mandays for the audit so that all features of the site and facilities can be considered. Consideration should be given to site vulnerabilities, neighbouring assets and the closeness of roads, rivers, and other access points etc.
* “Effective employees” are those individuals described in the organization’s management system and covered by the scope of the certification including non-permanent (seasonal, temporary, and sub-contracted) staff, whose work has the potential to affect security in the organization being audited. A certification body should agree with the organization to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/date and shift as appropriate.
* Part-time employees should be treated as full-time-equivalent employees. This determination will depend upon the number of hours worked as compared with a full-time employee, see 7 below for calculation of the impact of shifts. When calculating effective employees due consideration should be given to those persons whose work impact on supply chain security. E.g., Those employed in the finance department may not impact as much as those employed directly in manual processes.
* “Auditor time” includes the time spent by an Auditor or Audit Team planning (including off-site document review, if appropriate); interfacing with the organization and other relevant personnel, records, documentation and processes and report writing. It is expected that the “Auditor time” involved in such planning and report writing combined should not typically reduce the total on-site “Auditor time” to less than 80% of the time allocated for the audit. This applies to initial, surveillance and re-assessment audits. Where additional time is required for planning and/or report writing, this will not be justification for reducing on-site Auditor time. Auditor travel time is not included in this calculation and is additional to the Auditor time referenced in the chart.
* “Auditor time” as referenced is stated in terms of “Auditor Days” spent on the assessment. An “Auditor Day” is typically a full normal working day of 8 hours. The number of Auditor Days employed may not be reduced at the initial planning stages by programming longer hours per workday.
* During the first 3 years assessment cycle, Surveillance time for a given organization should be proportional to the time spent at initial assessment with the total amount of time spent annually on surveillance being about 1/3 of the time spent on the initial assessment. The planned surveillance time should be reviewed from time-to-time to account for changes in the organization, system maturity, etc., and at least at the time of re-assessment.
* The total amount of time spent performing the re-certification will depend upon the findings from reviews of the effectiveness of the management system and its implementation over the previous 3-year period. The amount of time spent at re-assessment should be proportional to the time that would be spent at initial assessment of the same organization and should be not less than 2/3 of the time that would be required for an initial assessment of the same organization at the time that it is to be re-assessed. Re-assessment is time spent above and beyond the routine Surveillance time, but, when re-assessment is carried out at the same time as a planned routine Surveillance visit, the re-assessment will suffice to meet the requirement for Surveillance as well.
* If a significant part of the operations is carried out in shifts, the total number of employees may be calculated as follows: (number of employees not in shift work) + (number of employees in shift work)(number of shifts minus one). This reduction can be applied providing there are no significant differences between the shifts with respect to the type and intensity of activities.
* Complexity should be derived from the number and type of operations undertaken. Risk should be derived from a qualitative assessment of risk affecting criteria such as: the potential security threats; types of, and likelihood that, products and /or services will be targeted; geographical location; local culture; history and trends of incidents; etc.
* An organization with one effective employee is an owner/operator. For example: truck owner operators who operate to systems such as those defined by International Road Transportation Union (IRU) Security Toolkit.

7.2.2 A full assessment of all ISO 28000:2007 requirements is mandated for any organization transitioning from an already existing ISO 9001 conforming system to ISO 28000:2007 system that was not previously assessed using qualified SCSMS 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 SCSMS 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 guidance in ISO 28003:2007, Annex B, Criteria for auditing organizations with multiple sites.

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 SCSMS 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 SCSMS, a certificate may be issued to the organization to cover all such sites provided that:

1. all sites are operating under the same SCSMS, which is centrally administered and audited and subject to central management review;
2. all sites have been audited in accordance with the organization’s internal security review procedure(s);
3. 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 SCSMS,
   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;
4. 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;
5. every site included in the SCSMS which is subject to significant threats to assets, vulnerabilities or impacts should be audited by the certification/ registration body prior to certification/ registration;
6. 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 SCSMS certification/ registration included in the Statement of Application;
7. 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 SCSMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

* 1. **Initial Stage 1 Audit**

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

1. general information concerning the SCSMS and activities it covers,
2. a copy of the SCSMS documentation including Statement of Application, Scope, Security Declaration(s), 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 SCSMS 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.

1. Results of the Stage 1 shall be documented in a written report.
2. SRI will review the report before deciding to proceed to the stage 2 audit and selection of team members with the necessary competence.
3. SRI makes the organization aware of the types of information and records required for examination at the stage 2 event.
   1. **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:

1. To confirm that the organization adheres to its own policies, objectives, and procedures;
2. To confirm that the SCSMS conforms to all the requirements of ISO 28000:2007 and is achieving the organization’s policy objectives;
3. Focus on:
   1. Supply Chain security risks,
   2. Documentation requirements from ISO 28000:2007, and ISO 28001:2007 as appropriate,
   3. Selection of security risk treatments and controls based on the risk assessment and risk treatment process,
   4. Review the effectiveness of the SCSMS, verification of the effectiveness confirmed through test and/or observation of the performance of the supply chain security system and controls, and review of the achievement of SCSMS objectives,
   5. Internal SCSMS Audits and Management Reviews (at least one full cycle of internal audits and management reviews performed),
   6. Management responsibility for the supply chain security policy,
   7. Correspondence between selected and implemented controls, the Statement of Application, results of the risk assessment and risk treatment process, and SCSMS policy and objectives,
   8. Implementation of controls and risk treatments,
   9. Programs, processes, procedures, records, internal audits, and reviews of the SCSMS effectiveness to ensure traceability to management decisions and the SCSMS policy and objectives.
4. Require the organization to demonstrate that the analysis of security related threats is relevant and adequate for the organization;
5. 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 SCSMS;
6. If documentation is combined with other management systems, the SCSMS 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 28000:2007 as a minimum, stating its conclusions on conformance and effectiveness of the supply chain security management system overall to the selected criteria. 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;

1. An account of the audit and summary of the documentation review;
2. An account of the organization’s supply chain security risk analysis including selection and implementation of effective risk treatment and controls;
3. Total time used, time spent on documentation, assessment of risk analysis, on-site audit, and audit reporting;
4. Audit enquires that have been followed, rational for their selection, and methodology employed;
5. 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 SCSMS 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 SCSMS, 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 SCSMS audits and management reviews, summary of observations regarding the implementation and effectiveness of the SCSMS, and a recommendation on whether the organization’s SCSMS 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 28000:2007 Audit Program (R20.23SCSMS). The audit program is established for each certificate cycle, at the start of the cycle.

1. Initial assessments shall cover the entire scope of the SCSMS as per the ISO 28000:2007 standard and other criteria.
2. Surveillance shall be conducted, as a minimum, once per year.
3. During a three-year period, the entire SCSMS must be assessed against the ISO 28000:2007 Standard with important/critical areas covered during surveillance in accordance with IAF Guidance.
4. 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 SCSMS standard;
5. Operational Requirements are those requirements identified by the organization and placed upon personnel that are “under the control” of the organization. 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.
   1. Other selected areas as appropriately prioritized for review;
   2. Effectiveness with regard to achieving objectives of the information security policy and security control implementations;
   3. Functioning of procedures for the periodic review of compliance with relevant legislation and regulations;
   4. Action taken on nonconformities identified during the last audit.
6. SRI will adapt its surveillance program to supply chain security issues as defined in the Statement of Application, SCSMS Scope, Security Declaration(s), and AEO criteria and requirements.
7. Use of the mark will be audited.
8. SRI will check the records of appeals and complaints and any failure to meet the requirements, and that the organization has investigated its own SCSMS 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 SCSMS 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:

1. The appropriate version of the ISO 28000:2007 Standard.
2. The assessment was performed in accordance with the requirements of ISO/IEC 17021-1:2015 and ISO 28000:2007.
3. Effective date and Expiration dates, with a maximum period of three years.
4. Scope of Registration.

7.8.4 If desired, separate certificates for the applicable ISO/IEC 27001:2013 and ISO 9001 may be issued.

7.8.5 All certificates shall be specific in terms of the scope of the SCSMS 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 Associate V.P., Certification, 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 28000, 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 28000:2007 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. There are requirements in excess of ISO/IEC 17021 pertaining to disciplinary actions that a CB must take if SCSMS auditors violate confidentiality or some other aspect of agreement concerning performance criteria under ISO 28003:2007. In addition, attention is required in regard to legal requirements for records retention (different depending on venue).

Some requirements in excess of ISO/IEC 17021; common criteria pertaining to confidentiality of information required for use in making management decisions and supporting operational CB processes, information made publicly available, and disclosure to third parties (except for that information discussed as above regarding specific SCSMS Confidential information). Significant requirements in excess of ISO/IEC 17021 pertaining to “..equipment/facilities that ensure the secure handling of confidential information (e.g. documents and records)..”.

SRI will provide facilities and equipment (examples may be documented and communicated “acceptable use” policies, lockable storage containers, encryption software, strong authentication mechanisms, etc.) and take special precautions regarding the receipt, storage, communication, access, disclosure, transmission, and destruction of information deemed to be confidential under this standard or as designated by Clients.

Some requirements in excess of ISO/IEC 17021 and ISO/IEC 19011; specific criteria for management system decisions, processes, and supporting evidence required pertaining to the communication of confidential information to third parties outside of the requirements of this standard or agreed upon procedures and arrangements. In some geographic venues, under legal and regulatory edict, information of certain types may require reporting of breach and disclosure to unauthorized individuals. For example: in the U.S., 44 states have legal and regulatory requirements for reporting of unauthorized disclosure or breaches of personally-identifiable information (such as Social Security Numbers, Personal Health Information, etc.) under the common legal construct of “State Breach and Disclosure Law”; European Union Directives have similar requirements and principles for reporting, as do other countries and jurisdictions.

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