SCS 9001 Certification Code of Practice

Document QF-040

September 23, 2026

Version 1.02

Revision History

Version	Date	Comments
1.0	January 9, 2026	Proposed final version.
1.01	January 20, 2026	Minor changes: • Miscellaneous changes after legal review • Addition of Section 8.5.4, Disputes clause • Enhancements to Section 7.1 Eligibility
1.02	September 26, 2026	Requirement CB-008 has been revised.

Table of Contents

Tables & Illustrations

1. Introduction

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents hundreds of global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs, standards development, and business performance improvement solutions, TIA 's members and participants are accelerating global connectivity across every industry and market.

TIA QuEST Forum brings together companies from around the world who operate modern networks and build products deployed within those networks. TIA volunteers develop certifiable, process-based industry standards to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA Quest Forum participants develop global standards that are supported by an extended ecosystem of organizations including industry, accreditation bodies, certification bodies, auditors and training professionals.

Within this document, the following abbreviations are frequently used:

- AB: Accreditation Body – an organization selected and authorized by TIA QuEST Forum to accredit Certification Bodies.
- CB: Certification Body – an organization accredited by an authorized AB to perform SCS 9001 certifications. Some industry publications refer to the CB as a Conformity Assessment Body. For the purposes of this document, they are identical.

TIA QuEST Forum standards are designed to be process-based and certifiable. The value of certification is to create public confidence and trust as established by an impartial and competent assessment by a third-party. It is the intent of TIA QuEST Forum to ensure that the SCS 9001 CoP builds confidence by ensuring that audits are consistently implemented and performed by competent auditors that are impartial, open and fair in their assessments.

The SCS 9001 CoP builds upon the requirements of ISO/IEC 17011 and ISO/IEC 17021-1 for ABs and CBs respectively and accordingly strives to remove redundant content from earlier versions of Code of Practice and associated documentation for simplification.

Further, this CoP aligns with the requirements of several International Accreditation Forum Mandatory Documents and the requirements stated therein are included in this CoP by reference and are identified in Appendix C: References.

1.1 Target Audience

This document is the TIA QuEST Forum SCS 9001 Code of Practice or CoP. It is intended as the authoritative document describing the SCS 9001 certification process. It is an aggregation of many prior process documents which represented the Scheme and Code of Practice for the TIA SCS 9001 Standard. All such contributing documents have been incorporated as relevant with prior versions no longer in use.

It may be helpful for the reader to define some terms:

- Scheme - the framework that defines how conformity to a standard is assessed, managed, and certified.
- Code of Practice (CoP) - requirements that individuals and organizations must meet in conforming to a standard.

This CoP has been developed for the benefit of:

- Certifying Organizations – to set expectations of the process and approach in preparing for certification
- Accreditation Bodies – to set the requirements necessary for TIA recognition to provide oversight of this CoP and for the accreditation of SCS 9001 CBs
- Certification Bodies – to set requirements for the execution of the CoP and required competencies
- Other Interested Parties – anyone with an interest in the TIA SCS 9001 CoP

This document is complemented by the publication QF-041 SCS 9001 Certification Guide. The Guide provides substantial additional material primarily for certifying organizations and has been developed in response to the many recurring questions raised on all aspects of the SCS 9001 certification process raised by interested parties.

1.2 The SCS 9001 Supply Chain Security Management System

The TIA SCS 9001 Supply Chain Security Management System (SCSMS) Standard is a cyber and supply chain security management system designed to address the growing risks of cyber-attacks in the supply chain of the information and communications technology (ICT) industry.

Developed by the Telecommunications Industry Association (TIA) members and participants, SCS 9001 is a certifiable, process-based standard that provides supply chain security protections for organizations in the ICT supply chain, including network operators, service providers, system integrators, resellers, and vendors. TIA works closely with the US government to ensure that SCS 9001 meets the needs of government and helps advance national security.

1.2.1 Acquiring the Standard

The SCS 9001 Standard may be purchased at the TIA QuEST Forum store E-Shop at: TIA QuEST Forum E-Shop. Preferred pricing is offered to TIA Quest Forum participants and volume discounts are available.

The Standard is also available from TIA's distributor Accuris. Accuris leverages its advanced platform to offer several attractive options including a cost-efficient floating license model.

See the Accuris site at TIA SCS 9001 | TIA Store for additional information

1.3 Contacting TIA QuEST Forum

For inquiries about this document or any other activity within TIA, the following contact information is provided:

1.3.1 Web Sites

- TIA web site: Telecommunications Industry Association | TIAonline.org | Home
- SCS 9001 web site: SCS 9001™ CYBER AND SUPPLY CHAIN SECURITY STANDARD - TIA Online

1.3.2 SCS 9001 Administrator Email

- SCS 9001 Administrator email address: supplychainsecurity@tiaonline.org

1.3.3 Mailing Address

Telecommunications Industry Association
QuEST Forum
1201 Wilson Boulevard, Floor 25
Arlington, VA 22209

2 Requirements of TIA QuEST Forum

TIA QuEST Forum is responsible for the development and on-going maintenance of this SCS 9001 CoP. TIA QuEST Forum shall fulfill its requirements detailed in the table which follows:

SCS 9001 TIA QuEST FORUM REQUIREMENTS	
Requirement	**Description**
TIA-001	Provide oversight of the SCS 9001 workgroup for the continued development and maintenance of the SCS 9001 Standard.
TIA-002	Continue to enhance and maintain this SCS 9001 CoP. Provide notifications to all impacted parties of planned changes to and availability of new versions of this CoP along with other updates and errata. Notifications shall be proactive and provided with sufficient lead time for interested parties to plan accordingly.
TIA-003	Provide supporting materials and a transition plan for future SCS 9001 releases.
TIA-004	Establish a central point of contact for all SCS 9001 certification related questions, issues and concerns from any party participating in SCS 9001 certifications.
TIA-005	Actively market and promote the Standard to drive industry awareness and to create business opportunities for AB, CB and training Organizations.
TIA-006	Define a process for the selection and authorization of ABs.
TIA-007	Establish contractual agreements with authorized ABs defining the agreed terms and conditions expected of ABs.
TIA-008	Recognize authorized ABs on the TIA QuEST Forum SCS 9001 web site.
TIA-009	Recognize accredited CBs on the TIA QuEST Forum SCS 9001 web site.
TIA-010	Recognize authorized training Organizations on the TIA QuEST Forum SCS 9001 web site.
TIA-011	Develop SCS 9001 program materials for the benefit of ABs, CBs and certifying organizations.
TIA-012	Collaborate with training Organizations to ensure training materials needed by ABs, CBs and certifying organizations are available. Advertise and promote training courses.
TIA-013	Develop and make available information and collateral to training Organizations to facilitate the development of associated courses. Collaborate with training Organizations in the development, review and release of training courses.
TIA-014	Develop and maintain information systems required in support of this SCS 9001 Code of Practice. An example is the Registration Management System (RMS), a platform used to manage certifications.

Table 1 - SCS9001 Code of Practice Requirements for TIA QuEST Forum

3 Requirements of SCS 9001 Accreditation Bodies (ABs)

The list of authorized ABs is maintained at: Audit Process - TIA Online.

SCS 9001 authorized ABs shall fulfill the requirements detailed in the table which follows:

SCS 9001 ACCREDITATION BODY REQUIREMENTS	
Requirement	**Description**
AB-001	Join TIA QuEST Forum as a Liaison participant. Active participation in the SCS 9001 workgroup is encouraged.
AB-002	Enter into an agreement with TIA QuEST Forum to accredit CBs for the SCS 9001 program meeting the requirements described herein.
AB-003	Be a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Agreement (MLA) for ISO 27001.
AB-004	Conform to IAF MD28:2023 Mandatory Document for the Upload and Maintenance of Data on IAF Database and updates as they become available.
AB-005	Accredit CBs per the requirements of ISO/IEC 17021-1 and other requirements as described herein.
AB-006	Consider recognizing the Witness Assessment of other authorized SCS 9001 ABs.
AB-007	Receive a written agreement from each accredited CB that all auditors will conduct SCS 9001 certifications in conformance with the requirements expressed herein.
AB-008	Perform Market Surveillance Audits for each CB audit that produces a Trigger 2 event.
AB-009	Upon an accredited CB's withdrawal or suspension, update the CB's record accordingly in the Registration Management System (RMS).
AB-010	Prior to accrediting a CB, conformance to the requirements stated herein will be confirmed through documentation review, witness assessments and office assessments.
AB-011	Assign personnel in support of SCS 9001 accreditations that have competence in the ICT industry, as well as in cybersecurity management systems.
AB-012	Assign AB assessors that have successfully completed and passed the exams for required SCS 9001 training. See Chapter Training.
AB-013	Perform an annual Witness Assessment for each CB that is accredited for SCS 9001. The witness audit may be for an Initial, Recertification or Surveillance Audit. The AB shall make every effort to observe different auditors during witnessing.
AB-014	Provide transition support for future SCS 9001 releases consistent with TIA QuEST Forum's guidance and transition plan.
AB-015	Provide notification to the TIA QuEST Forum Administrator of the date when each CB has successfully completed the Witness Assessment by updating the RMS.

AB-016	During the annual CB office assessment, the AB shall assess whether the CB has confirmed the competence of SCS 9001 auditors to conduct process-based auditing.
AB-017	Maintain an SCS 9001 accredited CB list, kept up-to-date and distributed to TIA QuEST Forum quarterly. This list shall note new additions or deletions from previous revisions. Notice of loss of accreditation shall be communicated promptly to the QuEST Forum Administrator.
AB-018	Inform TIA QuEST Forum of complaints received regarding the SCS 9001 program.
AB-019	AB assessors shall meet the requirements of IAF MD13.
AB-019	Conform to any additional requirements stated within this document.

Table 2 - SCS9001 Code of Practice Requirements for Accreditation Bodies

4 Requirements of SCS 9001 Certification Bodies (CBs)

The list of accredited CBs is maintained at: Audit Process - TIA Online. This list is not an endorsement by TIA of the companies listed. The listing simply demonstrates that a CB has met the criteria described below.

SCS 9001 accredited CBs shall fulfill the requirements detailed in the table which follows:

SCS 9001 CERTIFICATION BODY REQUIREMENTS	
Requirement	**Description**
CB-001	Join TIA QuEST Forum as a Liaison participant. Active participation in the SCS 9001 workgroup is encouraged.
CB-002	Be accredited to ISO/IEC 17021-1 and SCS 9001 certification by an authorized AB.
CB-003	Ensure auditors that perform SCS 9001 certifications meet the requirements of ISO/IEC 17021-1 Annex A *Required knowledge and skills* as well as the Qualification and Experience Requirements for SCS 9001 Certification Body Auditors described within this document.
CB-004	Provide ABs, as part of their accreditation and in advance of entering into a contract with a client to conduct SCS 9001 certifications, all appropriate documentation demonstrating that the CB's processes and business practices meet the requirements stated in this document.
CB-005	Maintain a current listing of SCS 9001 competent auditors.
CB-006	Utilize an audit team that includes at least one member with relevant experience in the Information and Communications industry.
CB-007	Have members of their management team with professional experience in the Information and Communications Technology industry.
CB-008	Ensure that the certification decision is made by personnel who are competent in the evaluation of management system audit results, independent of the audit team, and authorized by the CB to make certification decisions, in accordance with ISO/IEC 17021-1:2015 Section 9.5.
CB-009	Provide transition support for future SCS 9001 releases consistent with the TIA QuEST Forum's guidance and transition plan.
CB-010	Have at least one member of the certification decision making body who has successfully completed and passed the exams for required SCS 9001 training. This member shall have veto power regarding SCS 9001 certification decisions. See Chapter Training.

CB-011	Provide documented findings from the CB Audit Team at the end of each audit. The written report shall be provided to the certifying organization within 30 days of the conclusion of each audit, or within 45 days of the conclusion of a multi-site audit. The report will include the documented findings, overall audit conclusions, significant audit trails and recommendations.
CB-012	Conform to IAF MD28 Mandatory Document for the Upload and Maintenance of Data on IAF CertSearch Database and updates as they become available.
CB-013	If the CB supports multi-site audits, it shall do so by conforming to the requirements of IAF MD1:2023.
CB-014	If the CB supports integrated audits, it shall do so by conforming to the requirements stated in ISO/IEC 17021-1 and IAF MD 11:2023.
CB-015	Report all received complaints related to SCS 9001 certification activities to the TIA QuEST Forum Administrator.
CB-016	A Corrective Action Plan (CAP) for each nonconformity shall be received by the CB within 30 days following the Organization's receipt of nonconformity. This CAP shall include containment/correction, root cause analysis, corrective action and an implementation due date.
CB-017	An SCS 9001 certification shall not be issued until: (a) all major nonconformities are fully resolved; and (b) minor nonconformities are fully resolved or corrective action plans are defined with agreed resolution plans. A certified organization shall not receive recertification if there are overdue minor nonconformities from the previous audit or any unresolved major nonconformities at the time the certificate expires. Failure to meet the deadline for closing a major nonconformity after a surveillance audit shall lead to the suspension and potential withdrawal of the SCS 9001 certificate.
CB-018	Conform to the quarterly audit data reporting requirements and corrective action as described in Chapter Audit Data Collection & Reporting.
CB-019	Conform to any additional requirements stated within this document.

Table 3 - SCS9001 Code of Practice Requirements for Certification Bodies

5 Qualification Requirements of SCS 9001 Auditors

TIA QuEST Forum defines the qualifications for SCS 9001 Auditors. SCS 9001 auditor levels include the SCS 9001 Auditor and the SCS 9001 Lead Auditor. Individuals shall only participate in an audit at their presently qualified level. Both auditor levels have initial requirements and on-going maintenance requirements.

5.1 Requirements of the SCS 9001 Auditor

An SCS 9001 auditor evaluates and examines an organization's operations, processes, systems and records to ensure they conform with the Standard. They play a critical role in identifying risks, inefficiencies, or nonconformities.

The primary responsibilities of an auditor include:

- Planning Audits: defining objectives, scope, and methodology for the audit process.
- Collecting Evidence: reviewing documents, conducting interviews, and observing operations to gather information.
- Assessing Conformance: ensuring the organization adheres to relevant laws, standards, or guidelines (e.g., financial regulations or ISO standards).
- Identifying Risks: highlight potential issues that could impact the certification.
- Reporting Findings: prepare detailed reports with conclusions and actionable recommendations to address non-conformities and opportunities for improvement.

5.1.1 Initial Requirements of the SCS 9001 Auditor

The following lists the initial requirements of the SCS 9001 Auditor:

1. Complete the SCS 9001 Auditor training successfully.
2. Serve as the auditor for a minimum of one ISO/IEC 27001 full-system and two surveillance audits in the last three years, comprising at least twenty audit days during that period.
3. Meet the CB's requirements for process-based auditing approach.
4. Complete the CB's requirements for SCS 9001 Auditor.

5.1.2 Maintenance Requirements of the SCS Auditor

The following lists the maintenance requirements of the SCS 9001 Auditor:

1. Participate in at least three SCS 9001 audits per three-year period, commencing with the initial audit performed.
2. Complete a minimum of 2.0 CEUs in topics related to the cybersecurity or information security industries per three-year period.

5.2 Requirements of the SCS 9001 Lead Auditor

The SCS 9001 Lead Auditor is a professional responsible for overseeing and conducting audits to assess an organization's compliance with SCS 9001. The Lead Auditor leads the audit team, ensuring that the audit process is carried out efficiently and effectively. This role requires expertise in issues around cyber and supply chain security, strong leadership, and organizational skills.

Key responsibilities of the SCS 9001 Lead Auditor include:

- Planning and organizing the audit, including scheduling and setting objectives.
- Managing the audit team and delegating tasks.
- Conducting interviews, reviewing documentation, and gathering evidence.
- Preparing detailed audit reports with findings and recommendations.
- Ensuring impartiality and adherence to audit standards.

5.2.1 Initial Requirements of the SCS 9001 Lead Auditor

The following lists the initial requirements of the SCS 9001 Lead Auditor:

1. Meet all requirements for the Initial Requirements of the SCS 9001 Auditor.
2. Have met all CB requirements for Lead Auditor for a Management System Standard; and
3. Have met all CB requirements for SCS 9001 Lead Auditor.

5.2.2 Maintenance Requirements of the SCS 9001 Lead Auditor

The following lists the maintenance requirements of the SCS 9001 Lead Auditor:

1. Participate in at least six SCS 9001 audits per three-year period, with at least one being a full system audit.
2. Act as audit team leader in at least two of the six audits; and
3. Complete a minimum of 3.0 CEUs in topics related to the cybersecurity or information security industries per three-year period.

5.3 Training

TIA QuEST Forum offers comprehensive instructor-led training courses on a range of topics including an overview of requirements, implementation, and auditing. Course options include in-person on-site by the instructor or Virtual Instructor Led Training (VILT). VILT courses are scheduled and available based on demand.

These copyrighted courses are only available through TIA QuEST Forum Authorized Training Providers. At this time, Omnex is the exclusive SCS 9001 training provider.

Omnex's web site is: https://www.omnex.com/.

AB assessors and CB auditors are required to take the course and successfully pass the final exam:

Understanding and Auditing the SCS 9001™ Supply Chain Security Management System

This five-day course combines the pre-requisite Understanding SCS 9001 Requirements with SCS 9001 Auditor training to cover everything an auditor needs to know to audit the SCS 9001 Supply Chain Security Management System Standard.

A course synopsis, registration and cost information is available at: SCS 9001 Auditor Training | Auditing Supply Chain Security Management

5.4 Failure to Maintain Qualifications

A previously qualified auditor that fails to meet the maintenance requirements for their level shall be re-classified based upon the achieved qualifications. If requirements are not maintained, qualification shall be suspended. Qualifications for the lost classifications must be redemonstrated to be restored.

CBs have the responsibility to ensure auditor qualifications are confirmed for each three-year period.

6 Estimating the Time for Certification

The time for a certification can depend on many factors, such as:

- Organization: the complexity and maturity of the organization
- Scope: the size of the effort as driven by the defined scope
- Gap Analysis: an assessment of the organization's current practices and the amount of work to be done to close gaps to meet SCS 9001 requirements
- Gap Closure: implementing new policies to address gaps found during the gap analysis
- Preparation Time: the time to collect evidence, assemble a Pre-Audit Information Package, and support the audit.
- Audit Readiness: having assembled documentation for review by the CB and having employees available as needed

6.1 Core and Support Personnel

A basis for estimating the complexity of the SCSMS to be audited is the size of the organization associated with the SCSMS and the defined scope. That is, those that are responsible for defining, maintaining, tracking and executing the required processes within the defined scope.

The total number of employees within the scope is to be identified and defined as Core and Support personnel.

- Core Personnel: individuals with key roles and responsibilities for achieving the expected outcomes of the SCSMS including those responsible for planning, implementing, designing, managing, auditing, and providing input to the SCS 9001 process design.

  Core Personnel also includes individuals that plan, define requirements, design, test design, implement manufacturing controls and manage security processes for products and services within the defined scope.

- Support Personnel: individuals required to follow SCS 9001 processes and controls in the execution of their job function.

6.2 Determining Audit Duration

Forecasting anticipated audit days includes these steps:

1. Determine the headcount for Core and Support personnel.[1]
2. Enter the Core and Support headcount in the SCS 9001 Audit Duration Time Calculation Tool.

[1] The separation of Core and Support personnel is primarily for the purpose of calculating total audit time. Actual audit activities should be planned as needed with the required personnel.

3. An assessment is made of the certifying organizations' IT and systems complexity.

   The SCS 9001 Audit Duration Time Calculation Tool is used to calculate the expected baseline (minimum) audit days. The tool is available at: SCS 9001 Audit Duration Time Calculation Tool.

   There are other activities that will be considered to project the total amount of time an auditor is expected to spend on an SCS 9001 audit. TIA cannot influence the timing and duration of an audit. TIA does not set prices for any aspect of an audit and does not suggest rates for labor.

   Examples include:

   - Based on the impact of the factors qualifying the audit time, the CB determines whether an additional percentage of audit time is required and includes the justification for same in the SCS 9001 Audit Duration Time Calculation Tool.
   - Planning and audit report writing time is not included in the audit day calculation and requires additional time. Empirical evidence suggests that additional planning time is typically 25% of the calculated audit days and additional time for report writing is typically 15%.
   - An SCS 9001 Audit is distinct from other audits. Some organizations may elect to develop Integrated Management Systems. In such cases, the SCS 9001 Audit may be combined with other management systems such as ISO/IEC 27001, an information security management system.

As scheme owner, TIA manages the process described herein but it is not a Party to any Agreements between the AB, CB and certifying organization.

6.3 Business Complexity

Business complexity refers to the degree of difficulty, scale, risk, and diversity involved in an organization's operations that may impact its efforts in certifying its SCSMS. These factors are outside of the complexity of its information systems.

The following table provides categories and factors that impact the audit days determination.

Category	Factors Related to Business Complexity
Type(s) of business and regulatory requirements	1. The organization operates within non-critical or non-regulated sectors. 2. The organization has customers in critical business sectors. 3. The organization works in critical business sectors
Process and tasks	1. The organization has standardized processes with repetitive tasks; lots of people doing work under the org's control carrying out the same tasks; few products or services. 2. The organization has standardized but non-repetitive processes with a large number of products or services. 3. The organization has complex processes with a large number of products & services. It has many business units included in the scope of certification.
Level of establishment of the Management System	1. An ISMS is already well established and/or other management systems already in place. 2. Some elements of other management systems are implemented, others are not. 3. The organization does not have any other management systems implemented. An ISMS is new and not established.

Table 4 - Factors Related to Business Complexity

6.4 IT Complexity

IT complexity refers to the technical depth and diversity of an organization's IT environment — which directly impacts how complex and time-consuming it is to audit information and networking systems.

The following table provides categories and factors that impact the audit days determination.

Category	Factors Related to IT Complexity
IT Infrastructure Complexity	1. Highly standardized IT platforms, servers, operating systems, databases, networks, etc. 2. Several different IT platforms, servers, operating systems, dbases, networks. 3. Many different IT platforms, servers, operating systems, databases, networks etc.
Dependency on outsourcing & suppliers, including cloud services	1. Little or no dependency on outsourcing or suppliers. 2. Some dependency on outsourcing or suppliers, related to some but not all-important business activities. 3. High dependency on outsourcing or suppliers, large impact on important business activities.
Information System Development	1. None or very limited in-house system/app development. 2. Some in-house or outsourced system/app development for some important business purposes. 3. Extensive in-house or outsourced systems/application development for important business purposes.

Table 5 - Factors Related to the IT Environment Complexity

6.5 Qualifying Factors

Based upon the assessment of Business and IT Complexity, Qualifying Factors are the specific elements that help a CB adjust the base audit days according to the actual complexity and risk of the organization.

		IT Complexity		
		Low (3 - 4)	Medium (5 - 6)	High (7 - 9)
Business Complexity	High (7 - 9)	+5% to +20%	+10% to +50%	+20% to +100%
	Medium (5 - 6)	0%	0%	+10% to +50%
	Low (3 - 4)	0%	0%	+5% to +20%

Table 6 - Business & IT Complexity Audit Time Factors

6.6 Audit Duration Time

TIA QuEST Forum has developed an SCS 9001 Audit Days Table and associated SCS 9001 Audit Days Calculator to assist in estimating the number of actual audit days that can be expected.

The total audit duration will extend beyond this forecast of audit days. There will be preparation time, addressing reported nonconformities and on-going maintenance. TIA has no ability to forecast these types of efforts as they will be unique to the certifying organization.

6.7 The SCS 9001 Audit Days Table

An Audit Days Table is developed and refined based on empirical evidence of many prior certifications across many different standards. CBs use the Audit Days Table and other formulas, built from experience, which incorporate all factors to calculate the proposed number of audit days. These formulas include reductions based on requirement exclusions, integrated management systems, and multi-site reductions. It is a guideline with the amount of time for an audit ultimately determined by the CB and as negotiated with the certifying organization.

The SCS 9001 Audit Days Table has been developed for the exclusive application to SCS 9001 audits. It is based upon information within ISO/IEC 27006-1 with adjustments made for the introduction of CORE and SUPPORT Personnel, and real-world experiences of our CB Organizations of the audit times experience for ISO/IEC 27001.

While the audit days table is an effective starting point and provides guidelines for the anticipated number of audit days, the CB maintains considerable discretion in defining the expected duration of the audit based upon the Audit Days Table and other contributing factors including:

- the requirements of the relevant management system standard
- complexity of the client and its management system
- technological and regulatory context
- any outsourcing of any activities included in the scope of the management system.
- the results of any prior audits
- size and number of sites and their geographical locations
- the risks associated with the products, processes or activities of the organization
- whether audits are combined, joint or integrated
- special organizational circumstances

The most current table will always be available at Audit Process - TIA Online. At the time of publication of this document, the current table is provided below:

CORE Personnel Count	Audit Days	SUPPORT Personnel Count	Audit Days
1-10	5	1-10	.5
11-15	6	11-15	.5
16-25	7	16-25	1
26-45	8.5	26-45	1
46-65	10	46-65	1
66-85	11	66-85	1
86-125	12	86-125	1
126-175	13	126-175	1.5
176-275	14	176-275	1.5
276-425	15	276-425	1.5
426-625	16.5	426-625	1.5
626-875	17.5	626-875	2
876-1175	18.5	876-1175	2
1176-1550	19.5	1176-1550	2
1551-2025	21	1551-2025	2
2026-2675	22	2026-2675	2
2676-3450	23	2676-3450	2.5
3451-4350	24	3451-4350	2.5

4351-5450	25	4351-5450	2.5
5451-6800	26	5451-6800	2.5
6801-8500	27	6801-8500	2.5
8501-10700	28	8501-10700	3

Table 7 – SCS 9001 Minimum Audit Days Table

6.7.1 Audit Days Reduction

Certifications previously achieved including ISO / IEC 27001, ISO 9001 and / or TL 9000 may result in the reduction of audit days at the discretion of the CB. The assessment of SCS 9001 will be conducted per standard certification procedures for the requirements and controls in a currently valid release of the SCS 9001 Standard.

TIA QuEST Forum provides mapping tools demonstrating the equivalence of requirements and controls of SCS 9001 to the previously stated standards to assist the CB in determining the appropriateness of possible reductions.

6.7.2 Auditor Time

The SCS 9001 Auditor Time chart defines the minimum number of audit days needed to assess the SCS 9001 requirements.

The most current version of the table is available on the SCS 9001 website at Audit Process - TIA Online.

The table shows the minimum number of audit days that should be spent by the auditor for the SCS 9001 portion of the Initial Certification Audit (Stage 1 and Stage 2). The audit duration for recertification Audit, and ongoing Surveillance Audits can be reduced to two-thirds and one-third respectively. The number of days allocated for assessment of the SCS 9001 requirements must conform to the rules defined in the current SCS 9001 Auditor Time document for the initial or re-certification audit.

7 Conducting the Audit

7.1 Eligibility

Cybersecurity issues are driving global governments to enact new policies and regulations. In consideration of national security interests, the U.S. Federal Government and its various agencies have created a number of lists of foreign organizations subject to additional scrutiny for product and technology shipments up to the point of disallowing business relationships.

TIA QuEST Forum has aligned itself with these initiatives and taken a position to disallow entities identified by the U.S. Federal Government in certain of these lists to be certified to the standard or contribute to its further development.

The policy is described at: TIA-Policy-on-Government-Restrictions_040725.pdf.

The TIA QuEST Forum Registration Management System (RMS) is a database used to manage certifications. When an organization seeks certification, the process begins with the creation of a registration record within the RMS. Upon creation, this record is private and visible only to TIA, the certifying organization, it's selected CB, and the AB that accredited the CB. The record becomes publicly viewable upon successful completion of the audit and award of the SCS 9001 certificate.

The original creation of a registration record triggers a review process within TIA. The certifying organization is assessed against the then current version of the U.S. Government entity lists identified within the TIA policy. If the certifying organization is determined to be on one of the lists, then a notification correspondence is generated stating that fact with the determination that the organization is not permitted to proceed. Otherwise, a notification correspondence is generated that the registration is acknowledged and that the organization may proceed. The determination notifications are intended to be provided within 48 business hours of receipt of registration.

Entity lists are dynamic and subject to change from time to time. TIA will monitor these lists, and in cases whereby an organization is added to a list after a previous certification was approved and is in process, the organization and its CB will be notified of the change of status and that continuance is disallowed. In cases where the process was completed, and a certificate awarded, the organization will be notified of its change in status and that the certificate has been invalidated and the certification withdrawn.

An appeal can be made to the TIA Legal Counsel if the organization believes the determination has been made in error.

7.2 Registration Management System

The Registration Management System (RMS) is a platform developed and maintained by TIA QuEST Forum to manage certifications related to TIA QuEST Forum standards including SCS 9001. The RMS helps organizations register their conformance with TIA QuEST Forum standards and maintain and update their certification status.

Organizations that wish to become certified to SCS 9001 will first create a SCS 9001 Registration Profile in the Registration Management System (RMS). Each SCS 9001 registration has a 'private' Registration Profile that defines the organization's proposed parameters for eventual certification. Once the organization's registration is audited and certified, then a second profile is created in the RMS and made available to the public. This is the certified or public profile of the registration.

The CB shall enter required information in the IAF CertSearch database for accredited certificates. SCS 9001 certificates issued by a CB shall reference the SCS 9001 ID number assigned by the SCS 9001 Administrator when the Registration Profile is created.

The IAF CertSearch database is accessible at: IAF Certification Validation - IAF CertSearch.

CB auditors have access only to their SCS 9001 registered client accounts. They can check, validate and update all associated client information. CB administrators can see the private and public profiles for its SCS 9001 clients. The CB administrator can assign permissions for its auditors to also see them.

Once certified, an organization can edit their private registration profile, which is visible only to authorized registration administrators within the organization and their CB.

After certification, the organization can propose changes to the parameters of the certification by changing their private registration profile. Some of these changes will be immediately reflected on the public certified profile but most changes require approval by the Certification Body (CB) before the changes show to the public.

7.2.1 Creating a TIA QuEST Forum Account

Prior to creating a Registration Profile, users must first create an account with TIA QuEST Forum. Basic contact information is collected so that we may communicate with you. The link to access the TIA QuEST Forum portal and where new accounts can be created is at: QuEST Forum Portal Access.

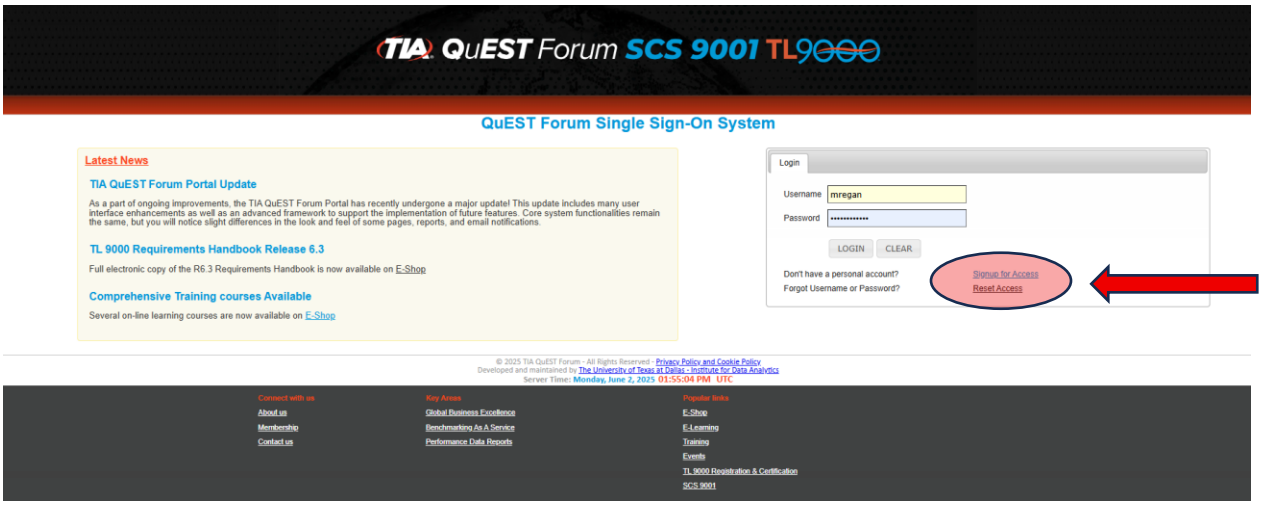

Illustration – TIA QuEST Forum Portal Access

7.2.2 Registration Profile

The information required for the Registration Profile is expected to be uniform across releases of the SCS 9001 Standard but may change from time to time. Organizations should review the Registration Profile requirements from the version of the SCS 9001 Standard to which it seeks certification and as described in the Standard in Chapter 4.3.2 – *Supply Chain Management System Profile and Scope* contains the requirements.

The profile includes various information such as:

- The organization and contact information
- The defined scope of the certification
- The release of the SCS 9001 Standard used for the certification
- The specific locations or sites relevant to the registration
- Requirements determined as not applicable
- NACE code(s)
- Principles of Trust (as described in SCS 9001, 4.2.3 – Collect and Report Corporate Principles of Trust)

7.2.3 Creating a Registration Profile

Creating a Registration Profile is a simple process. A high level introduction to the process is available at Getting Started - TIA Online.

The basic steps are:

1. Sign up for a new user account (if not previously created)
2. Create a new company record (if not previously created)
3. Login to the TIA QuEST Forum portal as a user
4. Create the new SCS 9001 registration, which includes entering the following information:

a. Section 1 – Profile Information
b. Section 2 – Profile Locations
c. Section 3 – Not Applicable Clauses
d. Section 4 – Profile Trust Principles
e. Section 5 – Review Profile Information

After initial creation, the user can access their registration through the TIA QuEST Forum portal for subsequent viewing / editing.

Detailed step-by-step instructions for creating a Registration Profile is available at: SCS 9001 Registration Creation. The Registration Profile is a public record. It is NOT available for public viewing until the audit is completed successfully, certification is granted, and the CB enables the record for public viewing. A Registration Profile for SCS 9001 will not be created if a company or individual appears on any government restricted lists as stated in the Policy.

7.3 SCS 9001 Pre-Audit Information Package

The SCS 9001 CB is required to obtain the information detailed in section SCS 9001 Pre-Audit Information Package. The information should be obtained within a mutually agreed timeframe prior to the commencement of the Stage 1 Audit. Having this information ensures an efficient audit and provides the CB with sufficient information to plan the audit. It is recommended that Surveillance and Recertification Audits be planned well in advance of their audit due dates.

The Pre-Audit Information Package is a collection of materials provided to auditors in advance of the Stage 1 audit and is a mandatory CB record. These materials provide auditors with an introduction to the certifying organization and a consolidated view of the current practices and controls in support of the organization's Supply Chain Security Management System (SCSMS). These materials facilitate the audit planning and help to identify major gaps prior to scheduling the Stage 2 Audit.

Providing a comprehensive, complete and accurate Pre-Audit Information Package will have a direct impact on effective audit planning.

7.3.1 Pre-Audit Information Package Aids

TIA QuEST Forum provides the following aids:

- SCS 9001 Pre-Audit Information Checklist: a checklist template to help in providing information and assembling mandatory information needed within the Pre-Audit Information Checklist.
- SCS 9001 Statement of Applicability (SoA) Matrix: a record of the SCS 9001 Annex A controls that are implemented and applied to asset types and justification for those that are not.
- SCS 9001 Clause Applicability Matrix: an organizing tool for both the certifying organization and its CB. It is provided to facilitate audit planning and the alignment of process elements.

7.3.2 Pre-Audit Information Package Mandatory Information

The following list details the information required in the Pre-Audit Information Package.

The CB shall provide to the organization:

- Instructions and Audit Process Guidelines: a cover letter or a detailed set of instructions is usually included to explain the audit process, timeline, and expectations. This part of the package clarifies what auditors will look for and provides contact details for any questions or further clarifications.

The organization shall provide to the CB:

1. The number of CORE and SUPPORT personnel within the scope.
2. Information required as detailed in SCS 9001 Chapter 4.3.1 - *Determining the Scope of the Supply Chain Security Management System*
3. Information required as detailed in SCS 9001, Chapter 4.3.2 – *Supply Chain Management System Profile and Scope*
4. Information required as detailed in SCS 9001, Chapter 4.3.3 – *Declaration of Requirement Applicability*
5. An SCS 9001 Statement of Applicability Matrix (SoA) as detailed in SCS 9001, Chapter 6.1.10 – *Organization's Statement of Applicability (SoA)*
6. An SCS 9001 Requirements to Process Mapping Matrix – the organizational process that fulfills each requirement and a Process Interaction Diagram (PID) that defines the processes to be evaluated and may include maps and flowcharts that identify key processes, highlighting decision points, inputs, outputs, and checks. This document may take different forms and be called different things including a 'turtle diagram' or "process map'.
7. An SCS 9001 Process to Site Mapping Matrix - a list of the processes executed at each site within the scope and accordingly to be audited.
8. Information of any recent and significant organizational changes, acquisitions, outsourcing activities or otherwise that may impact defined processes.
9. If the audit is a Surveillance or Recertification Audit, the organization may use the original Pre-Audit Information Package provided any subsequent changes are clearly identified.
10. A notation as to whether the organization is reporting the Annex B Measurements.
11. A list of all major outsourced business activities and associated entities.
12. Information on significant organizational changes, acquisitions, outsourcing or other significant changes that have occurred since the Certification Audit, if this is a Surveillance or Recertification audit.

7.4 Audit Criteria

The SCS 9001 CB shall:

1. If not an initial Certification Audit, the CB must confirm that the Pre-Audit information Package is still accurate.
2. Review the effectiveness of corrective actions. Sample system processes to include sampling of corrective actions that are overdue and corrective actions not considered overdue but are still open after nine months.
3. When reviewing documentation requirements, ensure that the current practice is reflected in the documented procedure and aligns with the applicable SCS 9001 requirement.
4. Review a sample of customer SCS 9001 audit findings and customer satisfaction results from the last SCS 9001 audit.
5. Follow-up on progress of any relevant formal complaints registered with the SCS 9001 CB against the organization.
6. Review root cause of security incidents to identify processes for additional focus within the audit.
7. If optional SCS 9001 Measurements are reported to the RMS, the audit shall confirm that that measurement collection, validation, and submittal was performed in accordance with SCS 9001 *Annex B Measurements*.

For those processes audited, the process review shall include an assessment of the effectiveness of that process.

7.5 Nonconformity Process

SCS 9001 CBs shall have a documented process to close major and minor nonconformities identified in a SCS 9001 audit report.

The process for closing nonconformities shall include:

- A Corrective Action Plan (CAP) for each nonconformity shall be received by the SCS 9001 CB within 30 days following the organization's notification of the nonconformity. This CAP shall include containment/correction, root cause analysis, and implementation due date. SCS 9001 CBs are required to respond to the proposed CAP in a timely manner. Resolution by the organization of a major nonconformity requires acceptable evidence of implementation of the CAP within the SCS 9001 CB's specified timeframe, not to exceed 90 days from the Organization's notification of the nonconformity.
- Resolution by the organization of a minor nonconformity requires acceptable evidence of completion of the CAP no later than the next scheduled audit. Exceptions to the resolution timeframes shall be approved by the CB and must be justified and documented.

- An SCS 9001 certification shall not be issued until: (a) all major nonconformities are fully resolved; and (b) minor nonconformities are fully resolved or corrective action plans are defined, reviewed and accepted.
- A certified organization shall not receive recertification if there are overdue minor nonconformities from the prior audit or there are open major nonconformities at the time the certificate expires.

Failure to meet the deadline for closing a major nonconformity after a Surveillance Audit shall lead to the suspension of the SCS 9001 certificate. Suspension may be lifted upon resolution of the nonconformity.

SCS 9001 CBs shall have a documented process to ensure that findings raised during audits have been documented, recorded and shared with the certifying organization. This process shall include an evaluation of the quantity and type of audit findings raised: majors, minors, and opportunities for improvements. The process shall include investigation and, where necessary, performance improvement of individual auditors who consistently misclassify audit findings.

7.5.1 Examples of Major Nonconformities

The following lists are examples of Major Nonconformities, but not an all-inclusive list.

- Demonstrably non-factual responses to the Principles of Trust questions.
- The omission of all aspects of a specific requirement of the SCS 9001 Standard.
- Systemic failure of the organization to implement and maintain effective internal audit and management review processes.
- Failure to achieve the intent of an SCS 9001 requirement.
- Failure to achieve the intent of an SCS 9001 control.
- Failure to comply with legal or statutory requirements.
- Multiple minor nonconformities within the same requirement, process, or part of the SCSMS which when considered in aggregate represent a breakdown of the organization's management system.
- Where CB judgment and experience can reasonably demonstrate the likelihood of failures of the SCSMS due to the inability to effectively implement SCS 9001 requirements, controls, or processes. Any such examples shall be fully documented and justified.
- Failure to correct minor nonconformities previously issued at the prior audit unless evidence is provided demonstrating progress towards an established implementation due date.
- If SCS 9001 Annex B Measurements are used, the repeated submission of data that is inconsistent with the counting rules described in SCS 9001 Annex B, or intentional lack of resubmissions of previous data when it is known to be inaccurate.

7.5.2 Examples of Minor Nonconformities:

The following lists are examples of Minor Nonconformities:

- An observed lapse in following a process, procedure, or the management system where judgment and experience can demonstrate there is minimal risk to the product and/or service being supplied.
- Any failure of the audited SCSMS to satisfy the effective implementation of a SCS 9001 requirement, control or process that is not considered to be a major nonconformity.

7.6 Multi-Site Certification

Multi-site audits are to be performed following the requirements of IAF MD 1 *Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization*.

IAF MD1 is for the audit and certification of management systems for organizations with more than one site managed by a single management system. Consideration is given to permissible sampling of sites as deemed sufficient by the CB.

7.7 Auditing of Virtual Sites

The SCS 9001 Management System may include a virtual organization or location(s). However, IAF MD4 states:

> *"A virtual site cannot be considered where the processes must be executed in a physical environment, e.g., warehousing, manufacturing, physical testing laboratories, installation or repairs to physical products."*

Further, when any audit, including that of a Virtual Site depends upon the use of ICT, the CB shall conform to IAF MD 4.

7.8 Disputes

TIA QuEST Forum is not a Party to Agreements between companies being certified and CBs providing certification services. ISO/IEC 17021-1 9.8 and 9.9 require the accredited CB to establish processes for handling complaints and appeals. Any disputes that may arise between companies during the Certification process are solely between the CB and the company seeking certification.

As the SDO and scheme owner, disputes related to interpretation of the intent of requirements are to be made to TIA Quest Forum by submitting questions through the Contact Us facility of the TIA QuEST Forum website. The question will be considered using appropriate subject matter experts. TIA QuEST Forum has a goal of providing a response within 10 business days of receipt which is to be considered final and accepted by all parties.

8 Activities After the Certification Audit

Issuance of Initial Certification is the outcome of a successful certification process, and it also begins the activities and expectations in maintaining an SCS 9001 certification. It is valid for a 3-year period. This section describes requirements after successful completion of the Certification Audit.

8.1 Audit Data Collection & Reporting

8.1.1 Introduction

TIA QuEST Forum is committed to the continuous improvement of its standards and operations, including associated certification processes. Through decades of experience in developing and providing oversight of the TL 9000 quality management system, certain performance expectations have been developed and have been adjusted as appropriate and extended to the SCS 9001 certification process.

Continuous Improvement depends on organizations implementing the SCSMS properly to effectively demonstrate conformance during all audits and that CBs demonstrate conformance to the SCS 9001 CoP.

Evaluating the effectiveness of SCS 9001 audits requires collecting data to determine the effectiveness of the SCS 9001 certification system. TIA QuEST Forum will aggregate that data and develop normative performance values for each measurement. Once normative performance values are determined, “Trigger Values” are determined which indicate deviation from the norm. The determination that a Trigger Value has been met is used to drive performance improvement activities.

CBs are required to provide the meta data outlined in this document. The data collected represents high level results of each audit and does not disclose any confidential information of the certifying organization. Further, the data is used strictly by TIA QuEST Forum in assessing CB performance and over-all improvements to the standard and this CoP.

As SCS 9001 is a new standard, the first goal is to collect results from a number of audits in order to have a sufficiently large data that is statistically meaningful. Until that time, the processes defined in Chapter 8.2 Triggers will not be implemented.

A notification of sufficient data having been collected in order to generate Triggers and initiate the corrective actions described within this document will be sent to all approved ABs and accredited CBs once attained.

8.1.2 TIA Responsibilities for Audit Data Collection & Reporting

TIA QuEST Forum provides the infrastructure for CBs to enter their collected data and has the following responsibilities:

- Evaluate the data provided by CBs as being complete and correct. Resolve if not.
- Enter the data into an internally developed evaluation workbook.
- Produce a variety of reports with examples CB results by accredited AB, regional results by all CBs, and specific CB results.
- Continuously assess Trigger Values and adjust based upon actual field data over time.
- Identify Trigger Values having been met.
- Provide notifications to interested parties.
- Engage with ABs for appropriate corrective action.

8.1.3 CB Responsibilities for Audit Data Collection & Reporting

TIA QuEST Forum requires CBs to provide data to analyze and identify patterns of performance of their audits. CBs are required to submit audit data to TIA QuEST Forum within eight weeks of the close of each calendar quarter.

Failure to do so shall result in immediate suspension by their Accreditation Body. The AB shall work with the CB to understand the reasons behind the lack of data submission and to implement corrective action prior to restoring the CB's status. Failure to do so will extend the CB suspension.

8.1.4 AB Responsibilities for Audit Data Collection & Reporting

TIA QuEST Forum will notify ABs if any of their accredited CBs having submitted data that causes a Trigger 1 or Trigger 2 to have been met. The AB shall report back to the TIA QuEST Forum with results of its investigation within 60 days of notification. Extensions to the investigation timeframe will be considered if requested.

8.2 Audit Data Collection Process

The steps below provide a high-level overview of the process used to collect, assess and report on audit data.

1. CB enters audit data into portal
2. TIA QuEST Forum creates a quarterly score card for review.
3. If no Triggers are reached, the CB is notified and the report is saved as a record by the CB.
4. If a Trigger 1 condition is met, the AB is requested to investigate the CB and report back to TIA QuEST Forum per 8.3.1.
5. If a Trigger 2 condition is met, the AB is requested to investigate and conduct a Market Surveillance per 8.3.2.

6. TIA QuEST Forum reviews and if accepted, acknowledges to AB per 8.3.1 and 8.3.2.

8.2.1 Data Submission Instructions

TIA QuEST Forum reviews this information to help determine how comprehensively SCS 9001 audits are being performed. It is understood that many SCS 9001 organizations are complex and constantly changing and utilize multiple processes as a result of acquisitions and consolidations. We review the reported nonconformities against audit day information to assess whether audits are utilizing only the minimum number of days in their assessments or are being expanded to cover the specific organizations' complexity.

Data required to be collected and reported by Certification Bodies on a quarterly basis includes:

- Number of Certification / Re-certification Audits
- Number of Surveillance Audits
- Number of certificates issued
- Number of major non-conformities
- Number of minor non-conformities
- Number of opportunities for improvement
- Number of Audit Days by Certification/Re-certification/Surveillance
- Minimum number of audit days per Certification/Re-certification/Surveillance

8.2.2 Failure to Submit Data

A series of escalating notifications are emailed when the CB data submission deadline has passed:

- The RMS automatically notifies all CB contacts to input audit data for the previous quarter. The email distribution list includes all the CB contacts who have permission to upload audit data, and copies other designated CB contacts.
- This first email notification is sent one month after the end of the quarter; as an example, for calendar Q1 (January through March), the email is sent by May 1st.
- If the data is not received, the RMS reminds the CB contacts to input audit data. The reminder notifies the CB to input data for the previous quarter as soon as possible and is sent to the CB contacts with a copy to the AB who accredited the CB. This second email is sent one day after the due date for the quarter.

If the CB has still not submitted the data, an email is sent to notify the AB with a copy to the corresponding CB to suspend the CB for missing audit data input. This suspension email is sent two weeks after the data due date.

8.2.3 Calculated Metrics

TIA QuEST Forum calculates the following metrics based on the raw data submitted by the CB:

- Major non-conformities reported per Audit (Initial, Surveillance, Recertification)
- Minor non-conformities reported per Audit (Initial, Surveillance, Recertification)
- Opportunities for Improvement reported per Audit (Initial, Surveillance, Recertification)
- Major non-conformities per Audit Day
- Minor non-conformities per Audit Day
- Opportunities for Improvements per Audit Day

The Major and Minor non-conformities reported per Audit are used to assess if a Trigger has been reached.

8.3 Triggers

A trigger value is essentially a predetermined threshold that, when reached or exceeded, initiates a specific action, process, and/or alert. In certifiable management systems such as TL 9000 or SCS 9001, and when applied to audit data, trigger values are used to identify potentially irregular auditing results. If the actual performance crosses this line, it "triggers" investigation or corrective action.

NOTE: a trigger having been raised does not necessarily indicate erroneous reporting data, it identifies an irregularity from expected norms that warrants investigation.

Trigger values are based upon the average number of all non-conformities, major and minor combined, per audit day. The sampling period is the trailing one-year period.

Trigger definitions are:

- Trigger 1 - the total number of non-conformities is 25% below the established norm.
- Trigger 2 - the total number of non-conformities is 40% below the established norm.

The TIA QuEST Forum continuously monitors submitted data and if appropriate, the normative levels and trigger values are adjusted as more empirical data from the field is acquired. If such a change is made, all program participants are notified.

In support of SCS 9001, two Trigger Values have been developed and are described in the next sections.

8.3.1 Trigger 1

Trigger 1 is the least severe of the triggers. Trigger 1 shall result in a request that the appropriate AB perform an investigation of the identified CB and report back a Root Cause Analysis, related actions and timeframes for completion of assigned corrective action to the CB. A response is required within one month of notification but the AB may request an extension of the investigation time if deemed necessary. The AB shall make such a request within 30 days of notification of the Trigger 1 condition.

8.3.2 Trigger 2

Trigger 2 is the more severe of the triggers. Trigger 2 indicates a much larger deviation from the norm and requires not only an AB investigation, but also a Market Surveillance Audit to be conducted. The Market Surveillance is used to further analyze the performance of the CB and the reason(s) for the irregular data.

When Trigger 2 is reached, TIA QuEST Forum shall notify the AB of the situation. The AB shall provide a plan for a Market Surveillance within 30 days. The AB may request an extension of time within the 30-day period if required. The AB shall conduct a Market Surveillance Audit within the following 60 days and submit a report to TIA QuEST Forum. TIA QuEST Forum shall review the report and identify any further actions within 5 days.

8.4 Performance Measurements for Benchmarking

Certain TIA QuEST Forum standards are differentiated through the value-added capability of industry measurements and benchmarking. This benchmarking system helps organizations improve their supply chain security management processes, enhance competitiveness, and ensure continuous improvement in their operations. Benchmarking enables certified organizations to compare their performance against industry standards and peers.

SCS 9001 administrators calculate Best-in-Class, Worst-in-Class, Industry Average, and Overall Average for each SCS 9001 measurement.

More information is available in the SCS 9001 Standard, Annex B2. *Measurements Processing, Usage and Responsibility Requirements.*

Currently, submitting measurements and participating in the SCS 9001 industry benchmarking program are optional.

8.4.1 Performance Data Reports

A Performance Data Report (PDR) is a benchmarking tool used in the SCS 9001 Supply Chain Security Management System to compare industry performance metrics. The reports are compiled from the data submissions by SCS 9001 certified organizations. The data is anonymized and securely kept in QuEST Forum's storage systems. There is no way to identify the organization submitting the data.

PDRs provide trend data and industry benchmarks across numerous measurement categories, offering insights such as:

- Best-in-Class performance
- Worst-in-Class performance
- Industry Average performance
- Monthly Average statistics

Available reports include:

- Performance Data Reports (PDRs): these reports contain industry benchmark data, allowing companies to assess their performance relative to others in the same sector. PDRs are available to TIA QuEST Forum participants at no charge and available for purchase by all others.
- Annual Performance Data: this report calculates the industry performance from the prior year. This report is available for free to SCS 9001-certified companies.

8.4.2 Auditing Considerations for Optional Benchmarking

If the organization participates in the optional benchmarking program, then the SCS 9001 auditor shall verify that all measurement processes are in place and effective to ensure the validity of SCS 9001 measurements.

The SCS 9001 Auditor shall verify that the organization has a documented system in place that covers, at least:

- Validation that SCS 9001 measurements are being collected and reported as required.
- Measurements can be validated as accurate.
- Measurements are used internally by the organization including management reviews of results and trends meeting set objectives with corrective action plans for results deviating from the organization's defined objectives.

If current performance shows an undesirable deviation from the organization's defined strategic objectives for SCS 9001 measurements, the auditor shall verify that corrective action has/is being taken, is documented, and progress is being tracked.

Auditors shall review the actual data submissions and verify proper implementation of the counting rules for required measurements.

For the initial Certification Audit, pre-certification data submissions require verification by the audit team.

When an Organization upgrades its registration to a new version of the SCS 9001 Standard as part of its Surveillance or Re-certification Audit, at least the most recent quarterly data submission shall use the new version of the Standard. SCS 9001 CB auditors will verify that all relevant counting rule changes have been properly implemented for the required measurements.

While the sample size for the above requirement is left to the SCS 9001 CB, it is expected that the depth of assessment for the sampled measurements assures accurate and comprehensive calculation, counting rules, reporting mechanisms, and validation of the measurements.

8.4.3 Late Data Submission Process

Content for this section will be provided at a later time if SCS 9001 benchmarking / measurements becomes mandatory.

8.4.4 Data Handling While Under Suspension

Content for this section will be provided at a later time if SCS 9001 benchmarking / measurements becomes mandatory.

8.5 SCS 9001 Certificate Suspension

After the award of the SCS 9001 certificate, there are certain circumstances that may lead to the suspension and potential withdrawal of the certificate. In addition to the suspension examples identified in ISO/IEC 17021-1, additional conditions for suspension include:

- The certified organization is acquired by another that is on a FCC's Covered List. See **Error! Reference source not found.**.
- The certified organization fails to submit measurements data for benchmarking if such a requirement becomes mandatory and not optional.

8.5.1 Measurements Data Treatment While Under Suspension

When an organization's certification is placed on suspension, any data submissions or resubmissions for that certification will be marked as "Not Certified". This means data can still be submitted and or resubmitted, but that data is not included in the PDRs.

When the certification is returned to "Certified" status, future data submissions will be included in the PDRs. Should the organization wish to have data submitted during the suspension period included in the PDRs, the data must be resubmitted after the certification has been reinstated.

8.5.2 Removing a SCS 9001 certification from suspension:

The CB can remove a certification from suspension if corrective actions have been taken that addresses the reasons for the suspension.

8.5.3 Withdrawal

If 90 days after a certification is placed on suspension, corrective action has not been taken to remove the suspension, then that certification will transition from being suspended to being withdrawn. This means the certification profile will not be visible to the public. If the organization wishes to attain certification, the initial certification process will apply.

Appendix A: Acronyms

Acronym	Meaning
AB	Accreditation Body
CAB	Conformity Assessment Body
CAP	Corrective Action Plan
CASCO	ISO Committee on Conformity Assessment
CB	Certification Body
CEU	Continuing Education Unit
CoP	Code of Practice
IAF	International Accreditation Forum
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMS	Integrated Management System
ISMS	Information Security Management System
ISO	International Organization for Standardization
MLA	Multilateral Recognition Arrangement
PDR	Performance Data Report
PID	Pre-audit Information Document
QMS	Quality Management System
RMS	Registration Management System
SCSMS	Supply Chain Security Management System
SDO	Standards Development Organization
SoA	Statement of Applicability
TIA	Telecommunications Industry Association

Appendix B: Definitions

Term	Definition
Accreditation Body	An organization that evaluates and determines whether certification bodies have demonstrated conformance in performing certification in accordance with defined standards.
Audit	A comprehensive evaluation of an organization's Management System to ensure it meets the requirements of a specific management system standard such as ISO 9001, TL 9000, ISO/IEC 27001 or SCS 9001.
Audit Days Table	A standardized reference used by certification bodies to estimate the number of days required to conduct a management system audit.
Audit Team	A group of individuals tasked with evaluating and assessing an organization's operations, systems, processes, or financial records to ensure they align with established requirements. They play a key role in identifying areas for improvement, uncovering risks, and assessing conformance.
Auditor	A professional that evaluates and examines an organization's operations, financial records, processes, or systems to ensure they conform with requirements. They play a critical role in identifying risks, inefficiencies, or errors and provide recommendations to improve overall performance and conformance.
Certification	A formal recognition that an organization has successfully met the requirements of a specific standard. The certification is granted by an independent certification body following a thorough audit process.
Certification Audit	The initial audit (Stage 1 and Stage 2) leading to a certification. Sometimes used interchangeably with Registration Audits.
Certification Body	An organization that is a specific type of conformity assessment body that provides third party certification services to assess and certify that products, systems, or organizations meet specific standards or requirements.
Code of Practice	A documented set of guidelines that outlines how individuals and organizations must behave to meet the requirements in conforming to a standard.
Conformity Assessment Body	A broad term for any organization performing conformity assessment activities (e.g., testing, inspection, certification). Sometimes used interchangeably with certification body.

Continuing Education Unit	A standardized measure used to document participation in professional development and training programs. It represents the time spent on education that helps professionals maintain or improve their skills, knowledge, or qualifications in their field.
Correction	An action to eliminate a reported nonconformity.
Corrective action	An action to eliminate the cause of a detected nonconformity or other undesirable situation.
Corrective Action Plan	A structured approach used to address and resolve problems, nonconformities, or deficiencies that arise within an organization. It outlines the steps required to identify the root cause of an issue, implement measures to correct it, and prevent it from recurring.
IAF CertSearch	A global database maintained by the International Accreditation Forum used to verify accredited management systems certifications.
Information and Communications Technology	Refers to any entity that implements, operates and administers a network, OR suppliers who provide the products and services used in such networks.
Information Security Management System	An Information Security Management System is a management system used to manage information and associated infrastructure. An example is ISO/IEC 27001.
Initial Audit	The first full audit conducted by a CB when an organization seeks certification for the first time. It includes both Stage 1 (Readiness Review) and Stage 2 (Certification Audit).
Integrated Management System	A framework that combines multiple management systems within an organization into a single, unified system. An example might be a security management system that includes both ISO/IEC 27001 and TIA SCS 9001.
International Accreditation Forum	A global association of accreditation bodies and other organizations involved in conformity assessment. Its goal is to develop a unified worldwide program to ensure that accredited certifications are reliable and recognized internationally.
International Organization for Standardization (ISO)	An independent, non-governmental organization that develops and publishes global standards including those to set requirements for organizations involved in auditing and certifying management systems.
ISO/IAF Action Plan	A collaborative initiative between ISO and IAF aimed at enhancing the credibility and effectiveness of certifications.

ISO Committee on Conformity Assessment (CASCO)	CASCO is a specialized committee within the International Organization for Standardization (ISO). Its primary focus is on developing policies and standards related to conformity assessment. Conformity assessment refers to the processes and activities used to ensure that products, services, systems, or organizations meet specified requirements.
Lead Auditor	A professional responsible for overseeing and conducting audits to assess an organization's conformance with specific standards or requirements. They lead the audit team, ensuring that the audit process is carried out efficiently and effectively. This role requires expertise in the audit's subject matter, strong leadership, and organizational skills.
Major Nonconformity	A nonconformity that affects the capability of the management system to achieve the intended results, the existence of which will disallow the award of a certification.
Market Surveillance Audit	A limited audit conducted by an AB to validate the findings of a CB auditor when requested by TIA QuEST Forum.
Minor Nonconformity	A finding that does not affect the capability of the management system to achieve the intended results
Multilateral Recognition Arrangement	An agreement established by the International Accreditation Forum to ensure mutual recognition of accreditation among its signatory members.
Nonconformity	Non fulfillment of a requirement.
Opportunity for Improvement	A finding that may identify areas for potential improvement in the organization’s management system but shall not include specific recommendations nor require action by the organization. Nonconformities shall not be recorded as opportunities for improvement.
Performance Data Report	A benchmarking tool used to compare organizational performance and trends against industry peers across a variety of metrics.
Pre-audit Information Package	Information provided by the Certifying Organization to the SCS 9001 CB prior to a scheduled Certification, Surveillance or Recertification Audit.

Quality Management System	A framework that organizations use to ensure that their products, services, or processes consistently meet customer and regulatory requirements. It focuses on improving quality, efficiency, and customer satisfaction through standardized processes and continuous improvement.
QuEST Forum Administrator	The person(s) responsible for oversight of TIA QuEST Forum activities.
Recertification Audit	An audit to confirm that an organization still meets the requirements of a certification standard before a certificate expires. For SCS 9001, a Recertification Audit is required every 3 years.
Registrar	Another term used for a certification body (CB) - an independent organization accredited to assess whether a company's management system complies with a specific standard.
Registration Audit	Used interchangeability with Certification Audit (See Certification Audit definition).
Registration Management System	A platform developed and maintained by TIA QuEST Forum to manage and oversee certifications and registrations related to TIA QuEST Forum standards including SCS 9001. The RMS helps organizations register their conformance with TIA QuEST Forum standards and maintain and update their certification status.
Registration Profile	A public record of information that describes the scope and other details of an organization's SCS 9001 certification.
Scheme	The framework that defines how conformity to a standard is assessed, managed, and certified.
Scope	When referring to a management system, the scope defines the boundaries and applicability of the system within an organization. It specifies what the management system covers, including the relevant activities, processes, products, services, locations, and organizational units. The scope ensures that all stakeholders understand what aspects of the organization are subject to the management system's policies, objectives, and controls.
SCS 9001 Administrator	The person(s) responsible for the TIA QuEST Forum SCS 9001 program.
Stage 1 Audit	A Stage 1 Audit is the initial phase of a certification audit process. Its purpose is to evaluate an organization's readiness for the more comprehensive Stage 2 Audit.

Stage 2 Audit	A Stage 2 Audit is the second and more detailed phase of the certification audit process, conducted after a successful Stage 1 Audit. The Stage 2 Audit assesses the implementation and effectiveness of the organization's SCSMS against the requirements of SCS 9001.
Standard Development Organization	A body responsible for creating, publishing, and maintaining standards that guide industries, technologies, and regulatory compliance.
Statement of Applicability	A document that lists which Annex A controls are applicable, and the rationale for inclusion or exclusion.
Supply Chain Security Management System	A framework designed to protect the integrity, security, and resilience of supply chains. It involves identifying risks, implementing security measures, and ensuring the safe handling of goods, data, and personnel throughout the supply chain.
Surveillance Audit	A scheduled review that takes place between Certification or Recertification Audits to ensure an organization is still in conformance.
Telecommunications Industry Association	A non-profit industry association and standards development organization that oversees the development and maintenance of global industry standards for the ICT industry including SCS 9001.
TL 9000	A Quality Management System developed in support of the Information and Communications Technology industry. The SCS 9001 CoP is modeled after many aspects of the TL 9000 program.
Trigger Value	A predetermined threshold that initiates a specific action, process, and/or alert. In certifiable management systems and when applied to audit data, trigger values are used to identify irregular auditing results that require investigation and potentially corrective action.
Validation Audit	An audit used to gather data to confirm the integrity of a certification process. Such audits typically sample randomly chosen, previously certified organizations for conformity to the requirements of a certification program.
Witness Assessment	An evaluation method where an AB observes an audit conducted by a certification body (CB) without interference to determine the audit team's competence to conduct the audit and to evaluate the effectiveness of the CB's audit program implementation.

Appendix C: References

Unless indicated otherwise, applicable references are to be the most recently approved and released versions.

- International Accreditation Forum (IAF) MD 1IAF Mandatory Document for the Audit and Certification of a Management System Operated by a Multi-Site Organization

  Document is accessible at: IAF MD1

- International Accreditation Forum (IAF) MD4: IAF MANDATORY DOCUMENT FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) FOR AUDITING/ASSESSMENT PURPOSES

  Document is accessible at: IAF MD4

- International Accreditation Forum (IAF) MD13: IAF MANDATORY DOCUMENT Knowledge Requirements for Accreditation Body Personnel for Information Security Management Systems (ISO/IEC 27001)

  Document is accessible at: IAF MD13

- ISO/IEC 17011 Conformity Assessment-Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies

  Document is available at : eStore ISO/IEC 17011:2017

- ISO/IEC 17021-1 Conformity Assessment-Requirements for Bodies Providing Audit and Certification of Management Systems Part 1: Requirements

  Document is available at : eStore ISO/IEC 17021-1:2015

- ISO/IEC 27001: Information security, cybersecurity and privacy protection — information security management systems — Requirements

  Document is available at: eStore ISO/IEC 27001:2022

- ISO/IEC 27006-1 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems Part 1: General

  Document is available at : eStore ISO/IEC 27006-1:2024

[This page intentionally left blank.]