

TIA Technical Bulletin

TIA QUEST FORUM'S SCS 9001 COMPARED TO ISO/IEC 20243

December 4, 2024

EXECUTIVE SUMMARY

Cybersecurity is a critical and sometimes confusing field of discussion that incorporates disciplines designed to protect digital assets, networks, and data from unauthorized access and cyber threats. There are many activities from standards development organizations, industry associations and government agencies to deliver new standards, recommendations and frameworks to address contemporary security challenges.

The sheer volume of activity can create uncertainty for organizations as to the benefits of many of these works and how they can be used in harmony to develop an effective and comprehensive security management system.

The purpose of this Technical Bulletin is to provide an introduction to the TIA SCS 9001 and ISO/IEC 20243-1:2023(E)[1] security standards, to provide an overview of their intended applications, and to contrast the differences between them[2].

The focus for each standard is the Information and Communications Technology (ICT) industry.

A FRAGMENTED INDUSTRY APPROACH TO SECURITY

There are many components of an effective security management system. Bad actors are conducting attacks of all types across all modern networks and the devices and services used to construct and operate those networks. Consideration of security is too often compartmentalized with a focus on a set of topics. Some examples include:

- **Network Security:** safeguarding the integrity of networks from intrusions and attacks.
- **Application Security:** securing applications through enhancement of software security.
- **Information Security:** protecting physical and digital data from unauthorized access, disclosure, and destruction.
- **DevSecOps:** evolving product development using agile methods that introduce security as a key consideration across the complete product development process.
- **End Point Security:** providing explicit controls to protect end points such as computers, cell phones and other network-connected devices.
- **Anti-Virus:** preventing the introduction of malware onto computing devices.
- **Operational Security:** addressing processes and introducing tooling into the administrative management of assets.
- **Supply Chain Security:** providing processes and tools to provide a higher level of assurance of the inherent security of products and services including assessing the operational practices of vendors.

Each of these topics play a pivotal role in forming a comprehensive defense strategy against the ever-evolving landscape of cyber threats. It is the position of TIA that to achieve material improvements to our cybersecurity defenses, all elements of security must be considered in a more holistic fashion.



INTRODUCTION TO THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA)

The Telecommunications Industry Association (TIA), the trusted industry association for the connected world, represents more than 400 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 and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI) and is active in developing and promoting international standards. TIA QuEST Forum brings together companies from around the world who manufacture, deploy and operate cutting edge networks, to develop process-based industry standards and tools to improve business performance and to address the challenges that come with digital transformation, new business models, innovation, and increasing competition.

TIA's QuEST Forum community developed and maintains the ICT industry's most prominent quality standard – TL 9000. As part of our commitment to ensuring global networks are reliable, trusted and secure, TIA QuEST Forum has released the "SCS 9001 Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS 9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry that also benchmarks performance to drive continuous improvement. This standard provides value to network operators of all types and developers and manufacturers of products and services used within those networks.

HISTORY OF ISO/IEC 20243



The history of ISO 20243 traces back to efforts of the Open Group Trusted Technology Forum (OTTF). The OTTF is a global initiative with support from industry, government, and other interested participants who collaborate to develop and evolve standards. The OTTF developed the Open Trusted Technology Provider™ Standard (O-TTPS) with the intent of helping technology providers build products with integrity and to enable customers to have confidence in the technology products they acquire. The O-TTPS addresses risks of maliciously tainted and counterfeit products in the ICT supply chain for Common Off the Shelf (COTS) products.

There are two distinct elements that should be understood with respect to this Standard: the O-TTPF (Framework) and the O-TTPS (Standard).

- **The O-TTPF (Framework):** the Framework is an evolving set of guidelines and best practices relating to the integrity of COTS ICT products and the security of the supply chain throughout the entire product life cycle. The Framework serves as the basis for the Standard, future updates, and additional standards.
- **The O-TTPS (Standard):** the Standard is a set of requirements, guidelines, and best practices intended to mitigate the risk of counterfeit and maliciously tainted products within the COTS product lifecycles. Coverage is provided for all product lifecycle phases - design, sourcing, build, fulfillment, distribution, sustainment, and disposal are accommodated.

The current version of the Standard was approved by The Open Group as Version 1.1.1 in 2018. It is believed that a new version is under development, but the release date has yet to be published.

ISO/IEC 20243 was approved for publication as an International Standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2015. It was named ISO/IEC 20243:2015. The standard has undergone revisions and updates to stay current with the evolving landscape of technology and security threats with new releases in 2018 and 2023.

The history and relationship between O-TTPS and ISO 20243 can be confusing. The standards each continue under development by their respective organizations, and each have a distinct certification path. They are very similar, in fact most requirements from the O-TTPS are repeated verbatim in ISO 20243. But there are subtle differences in requirement wording and additional requirements added in ISO 20243 that do not exist in the O-TTPS, at least at this time.

For the purposes of this Technical Bulletin, the standards are treated as technically equivalent. Descriptions which follow are taken from the O-TTPS with differences to ISO 20243 noted.

INTRODUCTION TO ISO/IEC 20243



ISO 20243 consists of two documents:

- *ISO/IEC 20243-1 - Information technology – Open Trusted Technology Provider Standard (O-TTPS) Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products.* This is the standard.
- *ISO/IEC 20243-2 – Information technology – Open Trusted Technology Provider Standard (O-TTPS) Part 2: Assessment procedures for the O-TTPS*. This document is a supplement and provides assessment procedures that may be used to demonstrate compliance with ISO 20243.

The goals of the standard are to address the perceived priority issues related to supply chain security and

defined as:

- Maliciously tainted product – products produced by the provider and acquired through a provider's authorized channel but have been tampered with maliciously.
- Counterfeit product – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

INTRODUCTION TO TIA SCS 9001

SCS 9001 defines requirements for implementation of a **Supply Chain Security Management System (SCSMS)**. It is a certifiable, process-based global standard with a specific focus on securing the supply chain of organizations operating in the Information and Communications Technology (ICT) industry. To secure the supply chain, an organization must demonstrate that it protects its sensitive information and IT infrastructure. Accordingly, SCS 9001 contains provisions to do so and presents itself as a super-set of the requirements.

As a process-based certifiable standard, SCS 9001 is designed to provide a framework for organizations to ensure that their processes consistently produce outcomes that meet organizational goals, customer requirements and may also be used to help conform with applicable regulations. Process-based standards are intended to help organizations improve efficiency, achieve operational excellence, and enhance customer satisfaction by adopting a systematic approach to managing and optimizing their processes. They emphasize the importance of understanding customer needs, establishing clear quality and security objectives, and implementing processes with a goal of continuous improvement. Certified organizations can demonstrate their commitment to quality and security, which can increase trust with customers and stakeholders.

As a process-based standard, SCS 9001 approaches the problem of supply chain security in a more powerful fashion by integrating the controls of other standards within its defined processes. These processes can be measured and continuously improved.

SCS 9001 was developed to provide an assessment of the security practices of network operators and their suppliers in delivering products and services of inherently higher security. A certification to SCS 9001 demonstrates that the organization practices comprehensive security policies; it is not used to certify a product or service.

SCS 9001 is used to provide higher assurance that vendors:

- are trustworthy,
- conduct all aspects of operations with a high level of security consideration,
- develop products and services with security built in from conception and considered throughout the entire product lifecycle,
- can demonstrate effective management of their own suppliers by ensuring the provenance of products and components from approved reputable sources,
- have made requisite investments to support products through their entire lifecycle, including the ability to more quickly identify, mitigate and resolve vulnerabilities found post-deployment.



COMPARISON OF SCS 9001 AND ISO 20243[3]

SCS 9001 and ISO 20243 are 149 and 31 pages in length, respectively. SCS 9001 is structured to conform to ISO Annex SL. ISO Annex SL, also known as the High-Level Structure (HLS), is a framework that provides a standardized structure for all ISO management system standards. It was introduced to ensure consistency and compatibility between different management system standards, making it easier for organizations to integrate multiple standards within their management systems. Annex SL imposes a universal structure with ten clauses, which include Scope, Normative References, Terms and Definitions, Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement. This unified structure facilitates the implementation, maintenance, and continual improvement of management systems, allowing organizations to streamline their processes and achieve better alignment with their strategic objectives. Interestingly, ISO 20243 is not structured to ISO Annex SL.

SCS 9001 organizes its requirements by the Annex SL clause. SCS 9001 also includes a list of Controls in an appendix, Annex A.

ISO 20243's requirements are organized around two themes:

- Technology Development: requirements applied to the product lifecycle, specifically product development.
- Supply Chain Security: requirements applied primarily to supply chain security of the product lifecycle.

Requirements are further organized under the Technology Development theme by identifying two distinct Methods:

- Product Development / Engineering Method: requirements to ensure a well-defined and repeatable product development process.
- Secure Development / Engineering Method: requirements to ensure security vulnerabilities are detected and fixed during the development process and mitigated when found post release.

The Supply Chain Security theme is limited to a single method, identified as the Supply Chain Security Method.

ISO 20243 provides a total of 86 requirements. **The following table provides the requirement count for each Method:**

ISO 20243 REQUIREMENTS BY METHOD	REQUIREMENTS
Product Development / Engineering Method	19
Secure Development / Engineering Method	21
Supply Chain Security Method	46

Table 1 – ISO 20243 Requirements

Only requirements and recommendations that address risks of tainted and counterfeit products are currently included in ISO 20243. As can be inferred from the sheer difference in the size of the standards, SCS 9001 offers a much more comprehensive set of requirements and controls in addressing not only the problems of maliciously tainted and counterfeit products, but many more considerations appropriate to determine if organizations can be viewed as trusted suppliers.

Accordingly, SCS 9001 includes a near-complete functional superset of the requirements of ISO 20243 while adding comprehensive support for many other requirements to more fully assess the organization's supply chain practices. These include areas of business process risk management which ISO 20243 deliberately avoids.

ISO 20243's requirements are succinct, usually a single sentence and analogous to other publications that present their requirements and recommendations as simple controls. SCS 9001 is a process-based standard that provides deep context into each required process including the needed to set Key Performance Indicators (KPIs) and to regularly evaluate performance against those KPIs with the goal of continuous performance improvement.

ISO 20243 does include more specific details in certain of its requirements, such as secure coding practices including setting compilation flags, desired product outcomes in hardware design, and product run-time protection capabilities.

REQUIREMENTS MAPPING BETWEEN SCS 9001 AND ISO 20243

The table which follows lists every ISO 20243 requirement and provides a mapping to the primary corresponding SCS 9001 requirement(s) and / or control[4].

ISO/IEC 20243-1:2023(E) Requirement		SCS 9001 Mapping
Product Development / Engineering Method (PD)		
PD_DES: Software / Firmware/Hardware Design Process		
PD_DES.01	A process shall exist that assures requirements are ad-dressed in the design.	8.3.2, 8.3.4
PD_DES.02	Product requirements shall be documented.	8.3.2, 8.3.4
PD_DES.03	Product requirements should be tracked as part of the de-sign process.	8.3.2, 8.3.4, 8.3.8
PD_CFM: Configuration Management		
PD_CFM.01	A documented formal process shall exist which defines the configuration management process and practices.	8.1.3, 8.1.4, 8.1.5
PD_CFM.02	Baselines of identified assets and artifacts under configuration management shall be established.	6.1.2, 8.1.5, 8.2.6
PD_CFM.03	Changes to identified assets and artifacts under configuration management shall be tracked and controlled.	8.1.3, 8.1.4, 8.1.5, SI-6
PD_CFM.04	Configuration management should be applied to build management and development environments used in the development/engineering of the product.	8.1.3, 8.1.4, 8.1.5[5]
PD_CFM.05	Access to identified assets and artifacts and supporting systems shall be protected and secured.	5.2.7, 5.2.8, 6.1.1, 8.3.4, 8.5.1
PD_CFM.06	A formal process shall exist that establishes acceptance criteria for work products accepted into the product baseline.	8.1.9, 8.3.4, 8.3.10, 8.3.12, 8.3.14, 8.4.3
PD_MPP: Well-Defined Development/Engineering Method Process and Practices		
PD_MPP.01	The development/engineering process as documented should be inclusive of development partners as defined by the governance process.	8.4.4
PD_MPP.02	The development/engineering process shall be able to track, as appropriate, components that are proven to be targets of tainting or counterfeiting as they progress through the life cycle.	5.2.13, 8.1.9, 8.3.10, 8.3.12, 8.4.3
PD_QAT: Quality and Test Management		
PD-QAT.01	There shall be a quality and test product plan that includes quality metrics and acceptance criteria.	8.3.6, 9.1.3
PD-QAT.02	Testing and quality assurance activities shall be conducted according to the plan.	8.3.6
PD-QAT.03	Products or components shall meet appropriate quality criteria throughout the life cycle.	8.3.6, 8.5.7

PD_PSM: Product Sustainment Management		
PD-PSM.01	A release maintenance process shall be implemented.	8.1.1, 8.6.1
PD-PSM.02	Release maintenance shall include a process for notifica-tion to acquirers of product updates.	8.2.4, 8.3.15, 8.4.4, 8.5.7, 8.6.1
PD-PSM.03	Release maintenance shall include a product update pro-cess, which uses security mechanisms.	8.1.1, 8.2.3, 8.3.2, 8.3.14, 8.3.15, 8.5.7
PD-PSM.04	A defect management process shall be implemented.	8.3.6, 8.3.14, 8.5.7
PD-PSM.05	The defect management process shall include a docu-mented feedback and problem reporting process.	8.3.6, 8.3.14
SE: Secure Development / Engineering Method		
SE_TAM: Threat Analysis & Mitigation		
SE_TAM.01	Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.	8.3.2, 8.3.5
SE_TAM.02	Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.	5.2.13, 8.1.9, 8.3.2, 8.3.5
SE_TAM.03	Threat analysis shall be used as input to the creation of test plans and cases.	6.1.6, 8.3.4, 8.3.6
SE_RTP: Run-Time Protection Techniques[6]		
SE_RTP.01	Run-time protection techniques as applicable to product architecture should be employed.	8.3.2, 8.3.5
SE_RTP.02	Run-time protection techniques should be included to mitigate the impact of vulnerabilities.	8.3.2
SE_RTP.03	Run-time protection techniques should be included to protect executable code against memory space, buffer overflow attacks, and null pointers.	8.3.2
SE_VAR: Vulnerability Analysis and Response		
SE_VAR.01	Techniques and practices for vulnerability analysis shall be utilized. Some techniques include: code review, static analysis, penetration testing, white/black box testing, etc.	8.3.2
SE_VAR.02	The impact of published vulnerabilities to products and processes should be analyzed and mitigated.	6.1.7, 6.1.8, 6.1.9, 8.1.3
SE_VAR.03	A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.	8.1.3, 8.2.4, 8.2.5
SE_VAR.04	Vulnerability analysis and response should feed into the processes for ongoing product development, product patching, and remediation.	6.1.6, 6.1.9, 8.3.16
SE_VAR.05[7]	This requirement is not in the OTTP-S[8].The requirement states that vulnerability analysis and response should be used for continuous improvement in the product development process.	8.1.3, 8.3.2, 10.2.1, 10.2.2

SE_PPR: Product Patching and Remediation		
SE_PPR.01	There shall be a well-documented process for patching and remediating products.	8.3.2, 8.7.1
SE_PPR.02	There should be a process for informing an acquirer of notification and remediation mechanisms.	8.1.3, 8.2.9, 8.2.4, 8.2.5, 8.4.4
SE_PPR.03	Remediation of vulnerabilities shall be prioritized based on a variety of factors, including risk.	8.3.2, 6.1.6, 6.1.7, 6.1.9
SE_PPR.04	Documented development and sustainment practices should be followed when implementing product remedia-tion.	8.3.2, 8.3.14
SE_SEP: Secure Engineering Practice		
SE_SEP.01	Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabili-ties. For example, user input validation, use of appropriate compiler flags, etc.	8.3.2
SE_SEP.02	Secure hardware design practices (where applicable) shall be employed. For example, zeroing out memory and effec-tive opacity.	8.2.8[9], 8.3.2
SE_SEP.03	Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.	7.2.1, 7.3.1, 8.1.9, 8.3.2, 8.3.3
SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape		
SE_MTL.01[10]	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.	6.1.6, 7.3.1
SE_MTL.02	Changes to the development/engineering practices, tools, and techniques shall be assessed in light of changes to the threat landscape.	8.3.2, 8.3.3, 8.3.14
SE_MTL.03	The cause of product vulnerabilities shall be evaluated and appropriate changes to the development/engineering practices, tools, and techniques identified to mitigate similar vulnerabilities in the future.	8.3.3, 8.3.14, 8.3.16, 8.7.1
Supply Chain Security Method (SC)		
SC_RSM: Risk Management		
SC_RSM.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.	6.1.6, 7.3.1
SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.	6.1.6, 6.1.7, 6.1.9
SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.	5.2.13, 6.1.9
SC_RSM.04	The output of risk identification, assessment, and prioriti-zation shall be addressed by a mitigation plan, which shall be followed routinely.	5.2.13, 6.1.9
SC_RSM.05	The mitigation plan should be reviewed periodically by practitioners, including management, and revised as appropriate.	5.2.13, 6.1.9
SC_RSM.06	Supply chain risk management training shall be incorporated in a provider's organizational training plan, which shall be reviewed periodically and updated as appropriate.	7.3.1, 8.1.9, 8.3.2, 8.3.3

SC_PHS: Physical Security		
SC_PHS.01	Risk-based procedures for physical security shall be estab-lished and documented.	4.1.1, 6.1.1, PE-1, PE-3, PE-4, PE-5, PE-6
SC_PHS.02	Risk-based procedures for physical security shall be fol-lowed routinely.	4.1.1, 6.1.1, PE-1, PE-3, PE-4, PE-5, PE-6
SC_PHS.03	Risk-based procedures for physical security should be re-viewed periodically by practitioners, including manage-ment, and revised as appropriate.	4.1.1, 6.1.1, PE-1, PE-3, PE-4, PE-5, PE-6
SC_ACC: Access Controls[11]		
SC_ACC.01	Access controls shall be established and managed for product-relevant intellectual property, assets, and arti-facts. Assets and artifacts include controlled elements re-lated to the development/manufacturing of a provider's product.	5.2.7, 5.2.9, 6.1.1
SC_ACC.02	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be documented.	5.2.7, 5.2.9, 6.1.13
SC_ACC.03	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be followed routinely.	5.2.7, 5.2.9, 6.1.1, 6.1.13
SC_ACC.04	Access controls established and managed for product-relevant intellectual property, assets, and artifacts should be reviewed periodically by practitioners, including man-agement, and revised as appropriate.	8.5.8
SC_ACC.05	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall employ the use of access control auditing.	5.2.8, 7.5.6, 8.3.6, AU-6
SC_ESS: Employee and Supplier Security and Integrity		
SC_ESS.01	Proof of identity shall be ascertained for all new employ-ees and contractors engaged in the supply chain, except where prohibited by law.	5.2.4
SC_ESS.02	Background checks should be conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities (within reason given local customs and according to local law).	5.2.4
SC_ESS.03	A set of business conduct guidelines applicable to its em-ployees and contractors should exist, consistent with prin-ciples embodied in industry conduct codes such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.	5.2.4[12]
SC_ESS.04	Business should be conducted in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.	4.2.3[13], 5.2.4, 8.4.1
SC_ESS.05	Periodic confirmation that suppliers are conducting busi-ness in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct, should be obtained.	4.2.3[12], 8.4.1, 8.4.4
SC_BPS: Business Partner Security		
SC_BPS.01	Supply chain security best practices (e.g., O-TTPS) shall be recommended to relevant business partners.	8.4.1[14], 8.4.3, 8.4.4, 8.4.5
SC_BPS.02	Legal agreements with business partners should reference applicable requirements for supply chain security practices (e.g., O-TTPS).	4.2.2, 5.2.4, 8.1.9, 8.2.7, 8.3.4, 8.4.1
SC_BPS.03	The provider should periodically request confirmation that business partners are following the supply chain security best practice requirements specified by the O-TTPS.	8.4.1[15], 8.4.3, 8.4.4, 8.4.5

SC_STR: Supply Chain Security Training		
SC_STR.01	Training in supply chain security procedures shall be given to all appropriate personnel.	5.2.2, 7.2.1, 7.3.1, 8.1.9, 8.3.2, 8.3.3
SC_ISS: Information Systems Security		
SC_ISS.01	Supply chain data shall be protected through an appropriate set of security controls.	7.5.3, 7.5.4
SC_TTC: Trusted Technology Components		
SC_TCC.01	The quality of supplied components shall be assessed against the component specification requirements.	8.3.10, 8.3.17, 8.4.6
SC_TCC.02	Counterfeit components shall not knowingly be incorporated into products.	5.2.13, 8.1.9
SC_TCC.03	Suppliers should be required to follow supply chain security best practices with regard to supplied components (e.g., O-TTPS).	5.2.13, 8.1.9, 8.3.17
SC_TCC.04	Vulnerability responses to affected supplied components should be jointly managed with the supplier.	8.1.3, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.6, 8.3.17
SC_STH: Secure Transmission and Handling		
SC_STH.01	Secure transmission and handling controls shall be established and documented.	5.2.12, CC-5
SC_STH.02	Secure transmission and handling controls shall be designed to lower the risk of physical tampering with assets and artifacts that are physically transported.	5.2.9, 5.2.12, 8.3.10, 8.5.10, CC-5
SC_STH.03	Secure transmission and handling controls shall be designed to lower the risk of tampering with assets and artifacts that are electronically transmitted.	5.2.9, 5.2.12, 8.3.10, CC-5
SC_STH.04	Secure transmission and handling controls shall be followed routinely.	5.2.9, 5.2.12, 8.3.5, 8.3.10, 8.4.7, 8.5.10, CC-5
SC_STH.05	Secure transmission and handling controls should be reviewed periodically by practitioners, including management, and revised as appropriate.	5.2.9, 5.2.12, 8.5.10, 9.3.2, 9.3.3
SC_STH.06	For assets and artifacts and related information that are considered to be high risk from the supply chain perspective, additional countermeasures, such as authenticity verification, should be employed.	5.2.13, 8.1.9, 8.2.8, 8.3.10, 8.5.10
SC_STH.07	Methods of verifying authenticity and integrity of products after delivery should be available.	4.1.1, 5.1.1, 8.1.9, 8.4.1, 8.4.6
SC_STH.08	***This requirement is not in the OTTP-S***[16]. The requirement states that there should be methods available to validate products after delivery.	8.4.3, 8.4.6
SC_OSH: Open Source Handling		
SC_OSH.01	Open Source assets and artifacts should be managed as defined by the best practices within the O-TTPS for Product Development/Engineering methods and Secure Develop-ment/ Engineering methods.	5.2.13, 6.1.6, 8.1.9[17]
SC_OSH.02	In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.	8.1.9, 8.3.10, 8.3.11, 8.4.3
SC_OSH.03	In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.	8.3.10, 8.4.3, 8.4.6
SC_OSH.04	For such sourced components, responsibilities for ongoing support and patching shall be clearly understood.	6.1.6, 8.1.3, 8.3.16, 8.4.1

SC_CTM: Counterfeit Mitigation		
SC_CTM.01	Instances of counterfeit activity relating to products shall be reviewed and an appropriate response sent.	5.2.13, 8.1.9
SC_CTM.02	Proper disposal procedures upon end of life should be employed (e.g., clearing data from hard drives, rendering a PCB non-functional, etc.) to protect from re-use in counterfeit product.	8.5.11, MP-4
SC_CTM.03	Practices should be deployed to preclude the unauthorized (counter-indicated) use of scrap from the hardware manufacturing process.	6.1.6, 8.4.3, 8.4.6
SC_CTM.04	Techniques shall be utilized as applicable and appropriate to mitigate the risk of counterfeiting, such as security labeling and scrap management techniques.	5.2.3, 5.2.9, 8.4.3, 8.4.6
SC_MAL: Malware Detection		
SC_MAL.01	One or more up-to-date malware detection tools	5.2.10, 5.2.11, 8.1.4, 8.2.8
SC_MAL.02	Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).	8.5.9

Table 2 – ISO 20243 Requirements Mapped to SCS 9001 Requirements & Controls

SCS 9001 CAPABILITIES BEYOND ISO 20243

SCS 9001 is a complete supply chain security management system for the ICT industry. Its intended application includes the supply chain security goals of ISO 20243 while providing substantial additional coverage to provide assurance of an organization's additional security and supply chain practices.

Some of the listed capabilities 'may' seem covered within ISO 20243, but when considered for the entirety of the organization involved in or having an influence of supply chain security, the example is deemed appropriate. As an example, ISO 20243 has requirements for access controls, but limited to systems involved that are 'product-relevant'. As another example, while ISO 20243 has requirements for managing parts, it does not expressly set requirements for Bills of Materials, which are becoming standard expectations within a supply chain security management system.

In the list below, the word 'security' is used as analogous to 'supply chain security'. Examples of SCS 9001 capabilities beyond ISO 20243 follow.

- Acceptable Use of Assets Policy
- Asset Classification
- Asset Inventory
- Asset Inventory DB and Management
- Asset Management Policy
- Audit Logging
- Bring Your Own Device (BYOD) Control Policies
- Business Continuity Planning
- Business Impact Analysis
- Corporate Principles of Trust
- Cryptographic Control Policies
- Customer Communication Methods

- Customer security requirements
- Data Sub-processors
- Design and Development Change Management Process
- Determining and Ensuring Workforce Competence
- Event and Incident Management Process
- Extent of Control of Critical Supplier(s)
- Hardware Bill or Materials (BOM)
- Human Resource (HR) Security Policy
- Identification of Customer and Stakeholder Security Needs
- Informing Customers of Security Design Changes
- Integration Planning
- Internal and external Communications
- Internal Audit Program
- Least Privilege Policy
- Maintenance of Organizational Systems
- Management of security objectives
- Management Responsibility for Supply Chain Security
- Media Management Policy
- Mobile Device Policy
- Monitoring Access Control
- Monitoring, measurement, analysis and evaluation
- Network Architecture Definition Process
- Network Security Requirements Definition Process
- Nonconformance records
- Notification of Critical Security Problems
- Notification of Critical Service Disruption
- Ownership of Assets
- Performance evaluation
- Problem Escalation
- Problem Report Feedback
- Product Replacement
- Release of products and services
- Required Security Measurements
- Requirements Traceability
- Residual Risk Information Availability
- Secure Development Models
- Secure Logistics Processes
- Secure Network Operations
- Secure Network Planning
- Secure Systems Operations
- Secure Systems Planning
- Secure Wireless Network Procedures
- Security Awareness Training
- Security Management System Evaluation
- Security Process Measurements
- Security Program Planning
- Security Requirements of Project Planning
- Software Bill of Materials (sBOM)
- Supplier Selection
- Supply Chain Security Operational Processes
- Supply Chain Security Risk Identification
- Supply Chain Security Risk Treatment
- Top management governance
- Verification of Externally Supplied Products
- Verification of Externally Supplied Services
- Workspace Policy
- Zero Trust Network Architecture

CONCLUDING REMARKS

ISO 20243 is a well written standard and one of the limited examples of a modern, purpose-built standard targeting the ICT supply chain. ISO 20243 does this with a focus on development and supply chain assessments focused on the integrity of parts and components.

As explicitly stated within the standard, its focus is:

> "...to enhance the security of the globally supply chain and the integrity of COTS ICT products..." and that it does so by providing "...a set of guidelines, requirements and recommendations that help assure against maliciously tainted and counterfeit products..."

These are certainly admirable goals which TIA also promotes and accordingly SCS 9001 accounts for essentially all ISO 20243 requirements. SCS 9001 builds upon ISO 20243 in providing an enhanced set of requirements and controls, delivered in a certifiable process-based standard, enabling an organization to evaluate a range of business processes of their suppliers.

SCS 9001 is a SUPPLY CHAIN SECURITY Management System (SCSMS), a new global standard with a focus on Supply Chain Security. SCS 9001 includes the goals of ISO 20243 in mitigating the risks of insecure products, but more importantly assesses the fuller security practices of organizations to provide evidence and documentation of steps that they have taken to become a reliable and trustworthy provider of secure products and services.

Security is a fragmented problem space and there is not a single security standard that accounts for everything needed to build a comprehensive security management system. All elements of security must be considered. As such, SCS 9001 and ISO 20243 can both be leveraged as part of a comprehensive security management system. The two standards can be used in harmony through integrated certifications for time and cost efficiencies and more powerful outcomes than using either standard in isolation.

REFERENCES

ISO 20243-1/2 - available for purchase on the ISO web site at: ISO - Search

Open Group Web site: About Us | www.opengroup.org

Open Group O-TTPS Standard: The Open Trusted Technology Provider™ Standard (O-TTPS) | www.opengroup.org

TIA SCS 9001 - available for purchase at: TIA SCS 9001 (accuristech.com)

Additional information regarding TIA's SCS 9001 Standard: TIA Supply Chain Security Program | TIA Online

FOOTNOTES

[1] In the balance of this document, ISO/IEC 20243-1:2023(E) will be referred to as ISO 20243.

[2] This content may include copyrighted materials from the Open Group and is used under the guidelines of 'fair use' for educational purposes.

[3] ISO 20243 is a copyrighted document, as is SCS 9001. Readers are encouraged to acquire copies of the standards for more detailed information related to the requirements and controls described within each publication.

[4] The SCS 9001 mapping is limited to the 3rd level of requirement specificity (e.g. 8.3.2 vs. 8.3.2.b). Note: the color coding of Methods and requirements is for readability and does not exist in ISO 20243.

[5] SCS 9001 does not limit the protections of organizational systems to development systems. All organizational systems used in support of the development of products and services are inferred within the requirements and controls.

[6] SCS 9001 is not as specific as ISO 20243 in specifying run-time protections designed within products. SCS 9001 infers such requirements in the establishment of a Secure Development Process but provides latitude to the organization on what specific requirements are to be established in consideration of the criticality of delivered products and services.

[7] This requirement was added in ISO/IEC 20243 and an equivalent requirement does not exist in OTTP-S. Accordingly, the textual description cannot be included as it is outside of the Open Group OTTP-S copyright.

[8] As the requirement is not in O-TTPS and has been introduced in ISO 20243, it cannot be repeated verbatim due to copyright restrictions.

[9] SCS 9001 sets a number of requirements for secure hardware design but does not include the two examples provided in SE_SEP.02.

[10] SE_MTL.01 and SC_RSM.01 appear to be the same requirement.

[11] SCS 9001 has a broad definition of 'assets' and expects all requirements to be applied regardless of whether the asset being protected is product-related, IT-system related, confidential information, or otherwise.

[12] SCS 9001 has a variety of requirements for human resource management, training, competency and conduct, but does not call out specific business conduct guidelines; this is inferred. Further, SCS 9001 does not define any requirements specific to the Electronic Industry Citizenship Coalition (EICC). The EICC is now known as the Responsible Business Alliance (RBA) and has a charter of improving social, environmental and ethical conditions in global supply chains. For additional information, see RBACodeofConduct8.0_English.pdf (responsiblebusiness.org).

[13] SCS 9001 has a set of requirements known as the Corporate Principles of Trust that requires certifying organization be transparent in disclosing specific information on their business practices as they relate to the Rule of Law.

[14] SCS 9001 takes a stronger position in requiring (not recommending) that suppliers meet expectation of security practices.

[15] SCS 9001 does not require providers to demonstrate adherence to the O-TTPS. The specific requirement is called out in O-TTPS. ISO 20243 generalizes the requirement listed O-TTPS as an example.

[16] As the requirement is not in O-TTPS and has been introduced in ISO 20243, it cannot be repeated verbatim due to copyright restrictions.

[17] SCS 9001 does not make direct reference to best practices defined with the O-TTPS but has its own comparable and in cases more detailed requirements for managing hardware, software and services from supply chain risk.

Disclaimer: The information and views contained in this article are solely those of its authors and do not reflect the consensus opinion of TIA QuEST Forum Participants or of the SCS 9001 workgroup. This bulletin is for information purposes only and it is intended to generate opinion and feedback so that the authors and TIA participants can learn, refine, and update this bulletin over time. The Telecommunications Industry Association does not endorse or promote any product, service, company or service provider. Photos and products used as examples in this paper are solely for information purposes and do not constitute an endorsement by TIA.

This document is not a Standard or TSB and does not modify any existing standards. This document is solely meant to communicate ideas and general information to industry.