Version: 0.4
Last Update: June 19, 2023

COMPARISON OF TIA QUEST FORUM'S SCS 9001 CYBER AND SUPPLY CHAIN SECURITY MANAGEMENT SYSTEM WITH ISO 28001

EXECUTIVE SUMMARY

This Technical Bulletin compares ISO 28001, the Security management systems for the supply chain with TIA's SCS 9001 Cyber and Supply Chain Security Management System.

ISO 28001 was introduced in 2007, reviewed and reconfirmed in 2012 and 2021 without change, meaning ISO has determined it to be sufficient in its original form for its intended use. It was prepared by Technical Committee ISO/TC 8, Ships and Marine Technology, in collabor ation with other relevant technical committees responsible for specific nodes of the supply chain.

SCS 9001 is a new standard, originally released in Q1 2022 with preparations for a second release targeted within H2 2023. SCS 9001 has been purpose-built to address today's cyber and supply chain security problems. It is a modern standard, developed by the Information and Communications Technology (ICT) industry and for the ICT industry.

When comparing against ISO 28001, SCS 9001 provides substantially more coverage and as appropriate to assess an organization's security practices. A detailed comparison of the two standards is provided below.

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 built 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 Cyber and Supply Chain Security Management System", a process-based standard focused on supply chain security for the global Information and Communication Technology (ICT) industry.

SCS9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the ICT industry and 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.

INTRODUCTION TO ISO 28001

ISO 28001 is a 34-page document detailing 31 requirements within its Performance Review List as contained in Annex A, Table A.1. Of the requirements, 15 or nearly 50% center on requirements for shipping, storage, cargo integrity, conveyance, transport routes and container security.

ISO 28001 identifies the requirements within its Performance Review List as 'Factors' and identifies the following primary areas:

1. Management of Supply Chain Security
2. Security Plan
3. Asset Security
4. Personnel Security
5. Information Security
6. Goods and Conveyance Security
7. Closed Cargo Transport Units

INTRODUCTION TO TIA SCS 9001

SCS 9001 is a Cyber and Supply Chain security standard developed by members of the ICT industry for the ICT industry.   SCS 9001 was developed to provide assurance of the proper operational hygiene of network operators and vendors in delivering products and services.

SCS 9001 was developed to help evaluate and provide higher assurance of upstream vendors so that they:

- operate their businesses with integrity and transparency and 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 through-out the entire lifecycle,
- 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 ISO 28001 TO SCS 9001

The following table provides excerpt from ISO 28001 Table A.1, identifying each Factor, requirement and adds a column providing commentary as to SCS 9001's level of equivalent coverage:

FACTOR	SCS 9001 COVERAGE
MANAGEMENT OF SUPPLY CHAIN SECURITY [2 REQUIREMENTS]	
Does the organization have a management system that addresses supply chain security?	SCS 9001 IS a supply chain security management system.
Does the organization have a person designated as responsible for supply chain security?	SCS 9001 provides a functional superset of requirements for organizational responsibilities and accountabilities.
SECURITY PLAN [3 REQUIREMENTS]	
Does the organization have (a) current security plan(s)?	SCS 9001 can be used in concert with a variety of legacy security standards with a more specialized focus, such as ISO 27001, an Information Security standard.
Does the plan address the organization's security expectations of upstream and downstream business partners?	SCS 9001 provides full coverage.
Does the organization have a crisis management, business continuity, and security recovery plan?	SCS 9001 provides a superset of these requirements.

ASSET SECURITY [5 REQUIREMENTS]	
Does the organization have in place measures that addresses: _ the physical security of buildings, _ monitoring and controlling of exterior and interior perimeters, _ application of access controls that prohibit unauthorized access to facilities, conveyances, loading docks and cargo areas, and managerial control over the issuance of identification (employee, visitor, vendor, etc.) and other access devices?	SCS 9001 provides extensive coverage of physical facility protections including those locations used for shipping and transportation of goods. Additionally, SCS 9001 identifies 12 controls associated with physical protection of all areas associated with supply chain security including but not limited to office space, related controls that must be implemented.
Are there operational security technologies which significantly enhance asset protection? For example, intrusion detection, or recorded CCTV/DVS cameras that cover areas of importance to the supply chain activity, with the recordings maintained for a long enough period of time to be of use in an incident investigation.	SCS 9001 identifies directly or makes inference to numerous 3rd party technologies and applications to be leveraged in meeting requirements. Physical security requirements do not explicitly call out CCTV/DVS cameras, but those requirements are inferred with the requirements of continuous monitoring. SCS 9001 goes beyond ISO 28001 in requiring monitoring to take place within many other corporate functions, such as network operations and access to critical IT assets.
Are there protocols in place to contact internal security personnel or external law enforcement in case of security breach?	SCS 9001 provides full coverage but does not explicitly call out notification to external law enforcement.
Are procedures in place to restrict, detect, and report unauthorized access to all cargo and conveyance storage areas?	SCS 9001 provides extensive coverage of physical facility protections including requirements for secure logistics. Additionally, SCS 9001 identifies 12 controls associated with physical protection of all areas associated with supply chain security.

Are persons delivering or receiving cargo identified before cargo is received or released?	SCS 9001 does not specifically call out that delivery persons are identified; if appropriate for a certifying organization, this expectation would be covered within other requirements of Secure Logistics.
PERSONNEL SECURITY [4 REQUIREMENTS]	
Does the organization have procedures to evaluate the integrity of employees prior to employment and periodically relative to their security duties?	SCS 9001 covers personnel consideration.
Does the organization conduct specific job appropriate training to assist employees in performing their security duties for example: maintaining cargo integrity, recognizing potential internal threats to security and protecting access controls?	SCS 9001 requires training of personnel.
Does the organization make employees aware of the procedures the company has in place to report suspicious incidents?	SCS 9001 requires personnel to report suspicions and concerns.
Does the access control system incorporate immediate removal of a terminated employee's company-issued identification and access to sensitive areas and information systems?	SCS 9001 requires elimination of access by terminated and retired employees.
INFORMATION SECURITY [7 REQUIREMENTS]	
Are procedures employed to ensure that all information used for cargo processing, both electronic and manual, is legible, timely, accurate, and protected against alteration, loss or introduction of erroneous data?	SCS 9001 provides for extensive information and data security protections, specific coverage of functions such as cargo processing would be accounted for as appropriate within the more general data protection requirements.

Does an organization shipping or receiving cargo reconcile the cargo with the appropriate shipping documentation?	SCS 9001 provides a variety of shipping and logistics protection requirements including the complete documentation of Chain of Custody (CoC) requirements including the authorized sequence of custody, control, transfer, and disposition of products during shipment.
Does the organization ensure that cargo information received from business partners is reported accurately and in a timely manner?	SCS 9001 provides a variety of shipping and logistics protection requirements including the complete documentation of Chain of Custody (CoC) requirements including the authorized sequence of custody, control, transfer, and disposition of products during shipment.
Is relevant data protected through use of storage systems not contingent on the operation of the primary data handling system (is there a data backup process in place)?	SCS 9001 provides full coverage with requirements for data backup, redundancy of critical systems, and business continuity plans.
Do all users have a unique identifier (user ID) for their personal and sole use, to ensure that their activities can be traced to them?	SCS 9001 provides a superset of coverage. As an example, SCS 9001 identifies a password lifecycle management process to manage personnel credentials and track access to assets.
Is an effective password management system employed to authenticate users and are users required to change their passwords at least annually?	SCS 9001 provides a superset of coverage. As an example, SCS 9001 identifies multi-factor authentication to be used for access to sensitive assets and a password lifecycle management process to ensure high quality passwords are used of sufficient complexity.
Is there protection against unauthorized access to and misuse of information?	SCS 9001 provides full coverage with extensive requirements for access to sensitive assets, including the logging and archival storage of records of such access.

GOODS AND CONVEYANCE SECURITY [6 REQUIREMENTS]	
Are procedures in place to restrict, detect, and report unauthorized access to all shipping, loading dock areas and closed cargo transport unit storage?	SCS 9001 provides full coverage of physical facility protections. Additionally, SCS 9001 identifies 12 controls associated with physical protection of all areas associated with supply chain security including but not limited to office space, related controls that must be implemented.
Are qualified persons designated to supervise cargo operations?	SCS 9001 has explicit requirements to ensure competence of all employees in their assigned job functions including contractors and third parties.
Are procedures in place for notifying appropriate law enforcement in cases where anomalies or illegal activities are detected or suspected by the organization?	SCS 9001 provides broad coverage for identification and notification requirements of security attacks but does not specifically require notification to law enforcement as a requirement. This would be an area for enhancement consideration as many governments have released or are considering legislation requiring notification of security attacks.
Are procedures in place to ensure the integrity of the goods/cargo when the goods/cargo are delivered to another organization (transportation provider, consolidation centre, intermodal facility, etc.) in the supply chain?	SCS 9001 provides a variety of shipping and logistics protection requirements including the complete documentation of Chain of Custody (CoC) requirements including the authorized sequence of custody, control, transfer, and disposition of products during shipment.
Are processes in place to track changes in threat levels along transport routes?	SCS 9001 has a requirement to only use approved shipping and logistics companies. It is our presumption that the responsibility for transport routes belong to the shipping company.
Are there security rules, procedures or guidance provided to conveyance operators (for example, the avoidance of dangerous routes)?	SCS 9001 has a requirement to only use approved shipping and logistics companies. It is our presumption that the expectations of conveyance operators would be accounted for in contracts.

CLOSED CARGO TRANSPORT UNITS [4 REQUIREMENTS]	
If a closed cargo transport unit is used, are there documented procedures for affixing and recording high security mechanical seals meeting ISO/PAS 17712 and/or other tamper-detection devices by the party stuffing the cargo unit?	SCS 9001 provides requirements for secure shipments including packaging, handling, storage, and transportation security requirements and anti-tamper methods such as shrink wrapping, use of security tape on boxes, pallet protections or other methods. SCS 9001 does not explicitly call out ISO/PAS 17712. This could be an area for enhancement if existing requirements are deemed inadequate.
If a sealed closed cargo transport unit is used, are there documented procedures in place to inspect seals for signs of tampering when the custody of conveyances changes during the course of a shipment and to address detected discrepancies?	SCS 9001 provides requirements for secure shipments including packaging, handling, storage, and transportation security requirements and anti-tamper methods such as shrink wrapping, use of security tape on boxes, pallet protections or other methods. This could be an area of improved requirement specificity if existing requirements are deemed inadequate.
If a closed cargo transport unit is used, is it inspected for contamination by the party stuffing immediately before stuffing?	SCS 9001 provides requirements for secure shipments including packaging, handling, storage, and transportation security requirements and anti-tamper methods such as shrink wrapping, use of security tape on boxes, pallet protections or other methods. This could be an area of improved requirement specificity if existing requirements are deemed inadequate.

If closed cargo transport units are used, are documented procedures in place for inspecting them immediately before stuffing by the party stuffing them to verify their physical integrity, to include the reliability of the unit locking mechanisms? A seven-point inspection process is recommended: _ Front wall _ Left side _ Right side _ Floor _ Ceiling/Roof _ Inside/outside closure _ Outside/Undercarriage	SCS 9001 provides requirements for secure shipments including packaging, handling, storage, and transportation security requirements and anti-tamper methods such as shrink wrapping, use of security tape on boxes, pallet protections or other methods. This could be an area of improved requirement specificity if existing requirements are deemed inadequate.

SCS 9001 COVERAGE BEYOND ISO 28001

SCS 9001 is a complete cyber and supply chain security management system for the ICT industry. It is a new standard, originally released in Q1 2022 with preparations for a second release taking place now with a target availability within H1 2023.

When comparing against ISO 28001, SCS 9001 provides substantially more coverage requirements to assess an organization's security practices.

SCS 9001 is approximately 150 pages in length. It contains 116 high-level requirements with most being multi-part. When fully considered, there are over 750 individual requirements.   Finally, SCS 9001 contains 60 controls and also specifies 7 measurements for those organizations electing to participate in TIA's Industry Benchmarking program.

Some examples follow in no particular order:[1]

[1] This is a partial list. SCS 9001 is a very comprehensive standard. Identifying and describing every requirement in detail is beyond the scope of this Tech Bulletin.

- Corporate Principles of Trust
- Zero Trust Network Architecture
- Asset Inventory DB and Management
- Understanding the needs and expectations of interested parties
- Relevant Legal, Statutory, Regulatory, or Contractual Requirements
- Leadership and commitment
- Top management governance
- Customer security requirements
- Establishing the security policies
- Media Management Policy
- Human Resource (HR) Security Policy
- Acceptable Use of Assets Policy
- Workspace Policy
- Access Control Policy
- Least Privilege Policy
- Asset Management Policy
- Mobile Device Policy
- Bring Your Own Device (BYOD) Control Policies
- Cryptographic Control Policies
- Counterfeit Parts Mitigation Policy
- Management Responsibility for Supply Chain Security
- Security Program Planning
- Asset Inventory
- Ownership of Assets
- Residual Risk Information Availability
- Asset Classification
- Supply Chain Security Risk Identification
- Security Risk Analysis
- Supply Chain Security Risk Treatment
- Business Impact Analysis
- Business Continuity Planning
- Management of security objectives
- People, Infrastructure, and Environment
- Monitoring, verification, and validation of resources
- Determining and Ensuring Competence
- Security Awareness Training
- Internal and external Communications
- Customer Communication Methods
- Organization Feedback
- Control of documented information
- Protection of Personally Identifiable Information (PII)
- Audit Logging
- Product Life Cycle Model
- Technical Vulnerability Management
- Secure Network Planning
- Secure Systems Planning
- Secure Wireless Network Procedures
- Maintenance of Organizational Systems
- Information Backup
- Problem Escalation
- Problem Report Feedback
- Product Replacement
- Notification of Critical Security Problems
- Notification of Critical Service Disruption
- Identification of Customer and Stakeholder Security Needs
- Design and development of products and services
- Secure Development Models
- Security Requirements of Project Planning
- Security Test Planning
- Integration Planning
- Requirements Traceability
- Security Test Verification and Validation Process Controls
- Software Provenance
- Software Bill of Materials (sBOM)
- Hardware Provenance
- Hardware Bill or Materials (BOM)
- Design and Development Change Management Process
- Informing Customers of Security Design Changes
- Security Vulnerability Resolution Configuration Management
- Component Substitutions
- Supplier Selection
- Data Sub-processors
- Supply Chain Provenance
- Extent of Control of Critical Supplier(s)
- Verification of Externally Supplied Products
- Verification of Externally Supplied Services
- Supply Chain Security Operational Processes
- Network Security Requirements Definition Process
- Network Architecture Definition Process
- Secure Network Operations
- Secure Systems Operations
- Event and Incident Management Process
- Incident Reporting
- Monitoring Access Control
- Software Malware Protection
- Secure Logistics Processes

- Disposal Process
- Release of products and services
- Control of nonconforming outputs
- Nonconformance records
- Performance evaluation
- Monitoring, measurement, analysis and evaluation
- Security Management System Evaluation
- Security Process Measurements
- Required Security Measurements
- Internal Audit Program
- Corporate Governance

CONCLUDING REMARKS

ISO 28001 is a narrowly focused standard for supply chain protection with a bias towards transportation and physical protection. With that intended purpose, it provides some useful protections. It was originally released in 2007 and hasn't changed since. Accordingly, it would not have been possible to account for the needs of the modern ICT industry and the types of cyberattacks and vulnerabilities that industry is now experiencing sixteen years later, and it does not.

SCS 9001 has been purpose-built to address today's cyber and supply chain security problems. It is a modern standard, developed by the ICT industry and for the ICT industry.

SCS 9001 goes far beyond the requirements of ISO 28001.

REFERENCES

- TIA's SCS 9001 Standard: TIA Supply Chain Security Program | TIA Online
- ISO 28001: available for purchase at ISO 28001:2007 - Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance (ansi.org)