TIA Technical Bulletin

TIA QUEST FORUM'S SCS 9001 SUPPLY CHAIN SECURITY MANAGEMENT SYSTEM EXPANDS UPON ISO/IEC 27001

September 23, 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 taking place from standards development organizations and global governments to produce new standards, recommendations and frameworks to address contemporary security challenges.

Considering the level of activity, organizations can be confused as to the purpose 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 introduce the SCS 9001 and ISO/IEC 27001 security standards, provide an overview of their intended applications, and to demonstrate the differentiation between them. ISO/IEC 27001 is an INFORMATION SECURITY Management System (ISMS), a global standard with a focus of Information Security. SCS 9001 is a SUPPLY CHAIN SECURITY Management System (SCSMS), a new global standard with a focus of Supply Chain 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 used to construct those networks. Consideration to security is too often compartmentalized with a focus on a limited set of themes, with examples including:

- **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 examples plays 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.

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.

INTRODUCTION TO ISO/IEC 27001 AND ISO/IEC 27002

ISO/IEC 27001 ("ISO 27001") is an international standard for managing information security. The title of the current version of ISO 27001 is:

"Information security, cybersecurity and privacy protection — Information security management systems — Requirements"

ISO 27001's origins trace back to the British Standard 7799, published in 1995 by the UK's Department of Trade and Industry. This standard was later adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), leading to the first publication of ISO/IEC 27001 in 2005. The standard has undergone several revisions, with significant updates in 2013 and 2022 (the current version), to address evolving information security challenges. It provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

ISO 27001 is supported by a companion document, ISO 27002, titled:

"Information security, cybersecurity and privacy protection — Information security controls."

ISO 27002 is a companion document and reference for selecting and implementing controls for information security risk treatment in an ISMS based on ISO 27001.

Unless specifically stated, and for simplicity, references to *"ISO 27001"* made within this Technical Bulletin shall be considered inclusive of both ISO 27001 and ISO 27002.

ISO 27001 defines the requirements for implementation of an **Information Security Management System (ISMS)**. It is a global standard with a specific focus of protecting **Information and IT infrastructure**. As such, it can be applied as an element of a comprehensive security management system.

As stated within the standard itself:

This document has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.

INTRODUCTION TO TIA SCS 9001

SSCS 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 and controls of ISO 27001. SCS 9001 is a powerful addition to the development and implementation of a comprehensive security management system.

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 was developed to help evaluate and 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 through-out the entire lifecycle,
- can demonstrate effective management of their own suppliers by ensuring the provenance of products and components from approved reputable sources in the final product,
- 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 27001[1]

As process-based certifiable standards, both SCS 9001 and ISO 27001 are designed to provide a framework for organizations to ensure that their processes consistently produce outcomes that meet customer requirements and comply 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 engaging in continuous improvement. By becoming certified, organizations can demonstrate their commitment to quality and security, which can increase trust with customers and stakeholders and create a competitive advantage.

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 is 149 pages in length. ISO 27001 and ISO 27002 are 26 and 164 pages in length, respectively. Both standards are constructed similarly as each conforms 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.

Both SCS 9001 and ISO 27001 define requirements within the body of their respective documents, organized by the Annex SL clause. Each document also includes a list of Controls in an appendix, Annex A.

The total requirements contained within each standard is provided in the following table[2]:

ANNEX SL CLAUSE	ISO 27001	SCS 9001
Chapter 4 Context of the Organization	10	52
Chapter 5 Leadership	17	134
Chapter 6 Planning	37	141
Chapter 7 Support	23	37
Chapter 8 Operation	9	386
Chapter 9 Performance evaluation	33	43
Chapter 10 Improvement	13	14
TOTAL	**142**	**807**

Table 1 – Comparison of Requirements Organized by Annex SL Clause

As previously stated, the intended use case for SCS 9001 is Supply Chain Security and ISO 27001 is Information Security. SCS 9001 is used by organizations to assess the trustworthiness of their suppliers in being able to consistently deliver inherently more secure products and services.

SCS 9001 has an expectation that assessed organizations have implemented an ISMS and build upon the ISMS with a great many additional requirements and specific controls focused on supply chain security. It is the belief of TIA that an organization that has not itself implemented information security controls within its own production and development environments cannot be a trusted supplier. Accordingly, SCS 9001 includes a near-complete functional superset of the requirements and controls of ISO 27001 as a fundamental baseline requirement while adding comprehensive support for evaluating the security of the organization's supply chain.

When considering the comprehension of SCS 9001, it is important to understand exactly what is being protected. As previously highlighted, ISO 27001 is an ISMS designed to protect information and IT infrastructure. SCS 9001 introduces the term 'asset', and it is organizational assets which SCS 9001 intends to protect.

As defined in SCS 9001:

An asset is anything that has value to the organization, whether it be physical or logical. Assets may be information, product-related, or key knowledge related to people. Assets shall be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.

The following table details the ISO Annex SL clauses, and the chapters and subchapters included within both standards. Upon inspection, the reader will notice the great many additional chapters and subchapters within SCS 9001 providing many requirements around all operational practices of the organization. It is this level of detail that is necessary to improve assurance that the operational practices of suppliers are sufficient to provide a high level of assurance of the inherent security of the organization's products and services.

ANNEX SL CLAUSE	ISO 27001	SCS 9001
Chapter 4 **Context of the Organization**	**4.1**–Understanding the organization and its context **4.2**–Understanding the needs and expectations of interested parties **4.3**–Determining the scope of the information security management system **4.4**–Information security management system	**4.1**–Understanding the Organization and its Context **4.1.1** Understanding the Organization and its Context **4.2**–Understanding the Needs and Expectations of Interested Parties **4.2.1** Interested Parties **4.2.2** Relevant Legal, Statutory, Regulatory, or Contractual Requirements **4.2.3** Collect and Report Corporate Principles of Trust **4.3**–Supply Chain Security Management System Scope **4.3.1** Determining the Scope of the Supply Chain Security Management System **4.3.2** Supply Chain Management System Profile and Scope **4.3.3** Declaration of Requirement Applicability **4.4**–Supply Chain Security Management System and its Processes **4.4.1** Process Based Supply Chain Security Management System **4.4.2** Documented Information of the Supply Chain Security Management System
Chapter 5 **Leadership**	**5.1**–Leadership and commitment **5.2**–Policy **5.3**–Organizational roles, responsibilities, and authorities	**5.1**–Leadership and Commitment **5.1.1** Top Management Governance **5.1.2** Customer Security Requirements **5.2**–Policy **5.2.1** Establishing the Security Policies **5.2.2** Security Policies **5.2.3** Media Management Policy **5.2.4** Human Resource (HR) Security Policy **5.2.5** Acceptable Use of Assets Policy **5.2.6** Workspace Policy **5.2.7** Access Control Policy **5.2.8** Least Privilege Policy **5.2.9** Asset Management Policy **5.2.10** Mobile Device Policy **5.2.11** Bring Your Own Device (BYOD) Control Policies **5.2.12** Cryptographic Control Policies **5.2.13** Fraudulent/Counterfeit Parts Mitigation Policy **5.3**–Roles, Responsibilities, and Authorities **5.3.1** Management Responsibility for Supply Chain Security **5.3.2**–Process Ownership **5.3.3**–Segregation of Duties

ANNEX SL CLAUSE	ISO 27001	SCS 9001
Chapter 6 **Planning**	**6.1**–Actions to address risks and opportunities **6.1.1** General **6.1.2** Information security risk assessment **6.1.3** Information security risk treatment **6.2**–Information security objectives and planning to achieve them	**6.1**–Actions to Address Risks and Opportunities **6.1.1** Security Program Planning **6.1.2** Asset Inventory **6.1.3** Ownership of Assets **6.1.4** Residual Risk Information Availability **6.1.5** Asset Classification. **6.1.6** Supply Chain Security Risk Identification **6.1.7** Security Risk Analysis **6.1.8** Establish the Acceptable Level of Risk (Risk Threshold) **6.1.9** Supply Chain Security Risk Treatment **6.1.10** Organization's Statement of Applicability (SoA) **6.1.11** Business Continuity Planning **6.1.12** Business Impact Analysis **6.1.13** Zero Trust Architecture (ZTA) Plan **6.1.14** Automation Planning **6.2**–Security Objectives and Planning to Achieve Them **6.2.1** Security Objectives **6.2.2** Management of Security Objectives **6.3**–Planning for Changes **6.3.1** Supply Chain Management System Changes
Chapter 7 **Support**	**7.1**–Resources **7.2**–Competence **7.3**–Awareness **7.4**–Communication **7.5**–Documented information **7.5.1** General **7.5.2** Creating and updating **7.5.3** Control of documented information	**7.1**–Resources **7.1.1** People, Infrastructure, and Environment **7.1.2** Monitoring, Verification, and Validation of Resources **7.2** Competence **7.2.1** Determining and Ensuring Competence **7.3** Awareness **7.3.1** Security Awareness Training **7.4** Communications **7.4.1** Internal and External Communications **7.4.2** Customer Communication Methods **7.4.3** Organization Feedback **7.5** Documented Information **7.5.1** General **7.5.2** Creating and Updating **7.5.3** Control of Documented Information **7.5.4** Access, Distribution, and Maintenance **7.5.5** Protection of Personally Identifiable Information (PII)

ANNEX SL CLAUSE	ISO 27001	SCS 9001
Chapter 8 **Operation**	**8.1**–Operational planning and control **8.2**–Information security risk assessment **8.3**–Information security risk treatment	**8.1**–Operational Planning and Control **8.1.1** Life Cycle Model **8.1.2** Security Risk Management **8.1.3** Technical Vulnerability Management **8.1.4** Secure Network Planning and Implementation **8.1.5** Secure Systems Planning and Implementation **8.1.6** Secure Wireless Network Procedures **8.1.7** Maintenance of Organizational Systems **8.1.8** Information Backup **8.1.9** Prevention of Counterfeit Parts **8.2**–Customer Communication and Requirements for Products and Services **8.2.1** Problem Escalation **8.2.2** Problem Report Feedback **8.2.3** Product or Service Replacement or Update **8.2.4** Notification About Critical Security Problems **8.2.5** Notification About Critical Service Disruption **8.2.6** Identify Stakeholder Security Needs **8.2.7** Security Contract Review **8.2.8** Hardware Design Requirements **8.2.9** Changes to Requirements for Products and Services **8.3**–Design and Development of Products and Services **8.3.1** Secure Development Models **8.3.2** Secure Development Process **8.3.3** Security Requirements of Project Planning **8.3.4** Security Requirements Definition Process **8.3.5** Product or Service Architecture Definition Process **8.3.6** Security Test Planning **8.3.7** Integration Planning **8.3.8** Security Requirements Traceability **8.3.9** Security Test Verification and Validation Process Controls **8.3.10** Software Provenance **8.3.11** Software Bill of Materials (sBOM) **8.3.12** Hardware Provenance **8.3.13** Hardware Bill of Materials (HBOM) **8.3.14** Design and Development Change Management Process **8.3.15** Informing Customers of Security Design Changes **8.3.16** Security Vulnerability Resolution Configuration Management **8.3.17** Component Substitutions **8.4**–Control of Externally Provided Processes, Products and Services **8.4.1** Supplier Selection **8.4.2** Data Sub-processors **8.4.3** Supply Chain Provenance **8.4.4** Extent of Control of Critical Supplier(s) **8.4.5** Critical Supplier Reviews **8.4.6** Verification of Externally Supplied Products **8.4.7** Verification of Externally Supplied Services **8.5**–Supply Chain Security Operational Processes **8.5.1** Network Security Requirements Definition Process **8.5.2** Network Architecture Definition Process **8.5.3** Secure Network Operations **8.5.4** Secure Systems Operations **8.5.5** Event and Incident Management Process

ANNEX SL CLAUSE	ISO 27001	SCS 9001
Chapter 8 **Operation**		**8.5.6** Incident Reporting **8.5.7** Change Management Process **8.5.8** Monitoring Access Control **8.5.9** Software Malware Protection **8.5.10** Secure Logistics Processes **8.5.11** Disposal Process **8.6**–Product Releases **8.6.1** Release of Products and Services **8.7**–Control of Nonconforming Outputs **8.7.1** Control of Nonconforming Outputs **8.7.2** Nonconformance Records
Chapter 9 **Performance Evaluation**	**9.1**–Monitoring, measurement, analysis and evaluation **9.2**–Internal audit **9.2.1** General **9.2.2** Internal audit programme **9.3**–Management review **9.3.1** General **9.3.2** Management review inputs **9.3.3** Management review results	**9.1**–Monitoring, Measurement, Analysis and Evaluation **9.1.1** General **9.1.2** Security Management System Evaluation **9.1.3** Security Process Measurements **9.2**–Internal Audit **9.2.1** Internal Audit Program **9.2.2** Internal Audits **9.3**–Corporate Governance **9.3.1** General **9.3.2** Corporate Governance Review Inputs **9.3.3** Corporate Governance Review Outputs
Chapter 10 **Improvement**	**10.1**–Continual improvement **10.2**–Nonconformity and corrective action	**10.1**–General **10.1.1** Improvement Opportunities **10.1.2** Employee Participation **10.2**–Nonconformity and Corrective Action **10.2.1** Nonconformity and Corrective Action **10.2.2** Supplier Corrective Action **10.3**–Continual improvement **10.3.1** Continual Improvement

Table 2 – ISO 27001 and SCS 9001 Requirements Organized by Clause and Subclause

ISO 27001 & SCS 9001 CONTROLS

SCS 9001 and ISO 27001 define 60 and 93 controls, respectively, as detailed in Annex A of each document. ISO 27001 controls are organized in support of the requirements detailed in Clauses 5 through 8. Table A.1 in ISO 27001 provides a simple description for each control. ISO 27002 describes each control in detail.

A count of the number of controls by Clause is provided in the following table:

ISO 27001 CONTROLS BY ANNEX SL CLAUSE	CONTROL COUNT
Section 5 – Organizational Controls	37
Section 6 – People Controls	8
Section 7 – Physical Controls	14
Section 8 – Technological Controls	34
TOTAL	**93**

Table 3 – ISO 27001 Controls

SCS 9001 organizes its controls by domain and is not aligned to Annex SL Clauses. A count of the number of Controls by Domain is provided in the following table:

ISO 27001 CONTROLS BY ANNEX SL CLAUSE	CONTROL COUNT
Management (AC)	4
Audits and Logs (AU)	6
Cryptography (CC)	8
Data Center (DC)	4
Identification and Authentication (IA)	7
Managed Maintenance (MA)	5
Media Protection (MP)	4
Physical and Logical Access (PE)	12
System and Information Integrity (SI)	7
System and Comms Protection (SP)	3
TOTAL	**60**

Table 4 – SCS 9001 Controls

It is important to note that the fact that SCS 9001 offers 60 controls in no way suggests the level of detail afforded by the standard is less than ISO 27001. SCS 9001 provides expansive coverage in the requirements of the standard in lieu of controls. SCS 9001 integrates controls within its requirements and processes, where they can be managed systemically with measurements and target results to identify areas of continuous improvement.

The table which follows lists every ISO 27001 control and provides a mapping to the primary corresponding SCS 9001 requirement and / or control.[3]

ISO 27001 CONTROL	SCS 9001 EQUIVALENT
5.1–Policies for information security	**4.4.2**
5.2–Information security roles and responsibilities	**5.2.4**
5.3–Segregation of duties	**5.3.3**
5.4–Management responsibilities	**5.1.1**
5.5–Contact with authorities	**8.5.5**[4]
5.6–Contact with special interest groups	**6.1.6**
5.7–Threat intelligence	**6.1.6**
5.8–Information security in project management	**6.1.1**
5.9–Inventory of information and other associated assets	**6.1.2**
5.10–Acceptable use of information and other associated assets	**5.2.5**
5.11–Return of assets	**5.2.4**
5.12–Classification of information	**5.2.9**

ISO 27001 CONTROL	SCS 9001 EQUIVALENT
5.13–Labelling of information	**5.2.9**
5.14–Information transfer	**5.2.5**
5.15–Access control	**5.2.7**
5.16–Identity management	**5.2.7**
5.17–Authentication information	**5.2.7**
5.18–Access rights	**5.2.7**
5.19–Information security in supplier relationships	**8.4.7**
5.20–Addressing information security within supplier agreements	**8.4.7**
5.21–Managing information security in the ICT supply chain	**8.4.7**
5.22–Monitoring, review and change management of supplier services	**8.4.5**
5.23–Information security for use of cloud services	**8.4.4**
5.24–Information security incident management planning and preparation	**8.5.5**
5.25–Assessment and decision on information security events	**8.5.5**
5.26–Response to information security incidents	**8.5.5**
5.27–Learning from information security incidents	**8.5.5**
5.28–Collection of evidence	**9.1.1**
5.29–Information security during disruption	**8.5.5**
5.30–ICT readiness for business continuity	**6.1.11**
5.31–Legal, statutory, regulatory and contractual requirements	**4.2.2**
5.32–Intellectual property rights	**4.2.2**
5.33–Protection of records	**7.5.4**
5.34–Privacy and protection of PII	**7.5.5**
5.35–Independent review of information security	**7.5**
5.36–Compliance with policies, rules and standards for information security	**7.5**
5.37–Documented operating procedures	**5.3.1, 6.1.11**
6.1–Screening	**5.2.4**
6.2–Terms and conditions of employment	**5.2.4**
6.3–Information security awareness, education and training	**7.3.1**
6.4–Disciplinary process	**5.2.4**
6.5–Responsibilities after termination or change of employment	**5.2.4**
6.6–Confidentiality or non-disclosure agreements	**5.2.4**
6.7–Remote working	**5.2.6**
6.8–Information security event reporting	**8.5.5**
7.1–Physical security perimeters	**PE-5**
7.2– Physical entry	**PE-1**
7.3–Securing offices, rooms and facilities	**PE-1**
7.4–Physical security monitoring	**PE-5**
7.5–Protecting against physical and environmental threats	**6.1.1, PE-6**
7.6–Working in secure areas	**5.2.6**
7.7–Clear desk and clear screen	**5.2.10, PE-12**
7.8–Equipment siting and protection	**7.1.1, 8.1.7, DC-1**

ISO 27001 CONTROL	SCS 9001 EQUIVALENT
7.9–Security of assets off-premises	**DC-2, MA-2**
7.10–Storage media	**5.2.3**
7.11–Supporting utilities	**6.1.1, DC-3**
7.12–Cabling security	**DC-3**
7.13–Equipment maintenance	**6.1.11**
7.14–Secure disposal or re-use of equipment	**8.5.11**
8.1–User endpoint devices	**5.2.6, 5.2.10**
8.2–Privileged access rights	**5.2.8**
8.3–Information access restriction	**5.2.7**
8.4–Access to source code	**IA-7**
8.5–Secure authentication	**8.5.8, IA-3**
8.6–Capacity management	**8.1.4, 8.1.5**
8.7–Protection against malware	**8.5.4, 8.5.9**
8.8–Management of technical vulnerabilities	**8.1.3**
8.9–Configuration management	**8.3.16**
8.10–Information deletion	**7.5.5, 8.5.11**
8.11–Data masking	**7.5.5**
8.12–Data leakage prevention	**6.1.6**
8.13–Information backup	**8.1.8**
8.14–Redundancy of information processing facilities	**6.1.11**
8.15–Logging	**8.1.5, 8.5.3**
8.16–Monitoring activities	**8.5.3**
8.17–Clock synchronization	**8.5.4**
8.18–Use of privileged utility programs	**5.2.8, 8.5.3, AU-3, IA-3**
8.19–Installation of software on operational systems	**8.1.5**
8.20–Networks security	**8.1.4, 8.5.1**
8.21–Security of network services	**8.1.5, 8.4.7**
8.22–Segregation of networks	**8.1.5**
8.23–Web filtering	**8.5.3**
8.24–Use of cryptography	**5.2.3, 5.2.9, CC1-8**
8.25–Secure development life cycle	**8.3.2**
8.26–Application security requirements	**5.2.10, 7.3.1, 8.1.5**
8.27–Secure system architecture and engineering principles	**8.3.2**
8.28–Secure coding	**8.3.1, 8.3.2**
8.29–Security testing in development and acceptance	**8.3.3, 8.3.6, 8.3.9**
8.30–Outsourced development	**8.4.4, 8.4.6, 8.4.7**
8.31–Separation of development, test and production environments	**8.1.5**
8.32–Change management	**8.1.4, 8.1.5, 8.5.7, 8.3.14**
8.33–Test information	**8.3.6**
8.34–Protection of information systems during audit testing	**9.2.2**

Table 5 – ISO 27001 Controls Mapped to SCS 9001 Requirements & Controls

SCS 9001 CAPABILITIES BEYOND ISO 27001

SCS 9001 is a complete supply chain security management system for the ICT industry. Its intended application includes the information security goals of ISO 27001 while providing substantial additional coverage to provide assurance of an organization's additional security and supply chain practices. In the list below, the word 'security' is used as analogous to 'supply chain security'. Examples of SCS 9001 capabilities beyond ISO 27001 follow.[5]

- Acceptable Use of Assets Policy
- Access Control 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
- Component Substitutions
- Control of nonconforming outputs
- Corporate Principles of Trust
- Counterfeit Parts Mitigation Policy
- Cryptographic Control Policies
- Customer Communication Methods
- Customer security requirements
- Data Sub-processors
- Design and Development Change Management Process
- Design and development of products and services
- Determining and Ensuring Competence
- Establishing the security policies
- Event and Incident Management Process
- Extent of Control of Critical Supplier(s)
- Hardware Bill or Materials (BOM)
- Hardware Provenance
- 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
- People, Infrastructure, and Environment
- Performance evaluation

- Problem Escalation
- Problem Report Feedback
- Product Life Cycle Model
- 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
- Security Risk Analysis
- Security Test Planning
- Security Test Verification and Validation Process Controls
- Software Bill of Materials (sBOM)
- Software Provenance
- Supplier Selection
- Supply Chain Provenance
- Supply Chain Security Operational Processes
- Supply Chain Security Risk Identification
- Supply Chain Security Risk Treatment
- Technical Vulnerability Management
- Top management governance
- Understanding the needs and expectations of interested parties
- Verification of Externally Supplied Products
- Verification of Externally Supplied Services
- Workspace Policy
- Zero Trust Network Architecture

CONCLUDING REMARKS

Cyberattacks and cyber-crime in general are increasing in complexity and harm to industry, organizations and consumers. It is estimated to cause $10.5 trillion a year in damage by 2025. (McKinsey, 'What is cybersecurity', 2023).

IBM Security publishes a report titled "The Cost of a Data Breach Report" and has done so for 18 consecutive years. Its purpose is to provide IT, risk management and security leaders with evidence to better manage security investments and risk management. The 2023 edition of the report evaluated 553 organizations impacted by data breaches which took place in the prior year and concludes the average cost of a breach was $4.45 million. This represents an increase of 15.3% from the 2020 report.

There are growing examples of both class action lawsuits and government legal action against companies and individuals deemed to have acted inappropriately in not establishing secure operating practices and insufficient behavior and cooperation during an attack.

Virtually all governments are becoming more active in demanding improved security in their communications networks and especially critical infrastructure. As an example, the U.S. Government published the National Cybersecurity Strategy in March 2023. The goals described therein are actively being pursued through a variety of measures. An important statement is provided in the STRATEGIC OBJECTIVE 3.3: SHIFT LIABILITY FOR INSECURE SOFTWARE PRODUCTS AND SERVICES, an excerpt of which states :

We must begin to shift liability onto those entities that fail to take reasonable precautions to secure their software *while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities.* ***Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care, they owe consumers, businesses, or critical infrastructure providers.*** *Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product. Doing so will drive the market to produce safer products and services while preserving innovation and the ability of startups and other small- and medium-sized businesses to compete against market leaders.*

The Administration will work with Congress and the private sector to develop legislation establishing liability for software products and services. *Any such legislation should prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios. To begin to shape standards of care for secure software development,* ***the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products*** *and services. This safe harbor will draw from current best practices for secure software development, such as the NIST Secure Software Development Framework. It also must evolve over time, incorporating new tools for secure software development, software transparency, and vulnerability discovery.*

Clearly, organizations must protect themselves and their customers from cyber-attacks.

The purpose of this Technical Bulletin is to demonstrate that SCS 9001 and ISO 27001 are important global standards, each developed for a different purpose. **ISO 27001 is an INFORMATION SECURITY Management System (ISMS)**, a mature, widely deployed global standard with a focus of Information Security. **SCS 9001 is a SUPPLY CHAIN SECURITY Management System (SCSMS)**, a new global standard with a focus of Supply Chain Security. SCS 9001 addresses an even more challenging security problem and includes essentially all capabilities of ISO 27001.

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 27001 can both be leveraged as part of a comprehensive security management system. SCS 9001 can be viewed as a functional super-set of ISO 27001. The two standards can be used in harmony through integrated certifications for time and cost efficiencies, leading to certificates being awarded for conformance to both.

In closing, **SCS 9001 is a process-based, certifiable global standard**. It describes how outcomes can be achieved through the implementation of its defined policies, processes, requirements and controls. It was developed to provide assurance that the providers of network products and services can be trusted, operate with a high level of integrity, and operate their businesses with a high level of transparency. It was developed to support of network operators of all types to evaluate their suppliers and to provide a higher level of assurance that their vendors:

- Are trustworthy,
- Conduct all aspects of operations and product development with a high level of security,
- Deliver products that are inherently higher in security and quality,
- Deliver consistent and reliable results, and
- 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.

In turn, all organizations can benefit with an SCS 9001 certification to:

- Improve its security posture to protect itself against cyber and supply chain attacks,
- Protect its brand and future business outcomes,
- Avoid potential litigation and class-action lawsuits,
- Demonstrate its security commitment to their own customers,
- Gain a competitive advantage by building a reputation as a trustworthy vendor, and
- Demonstrate its alignment to, and support of, other non-certifiable publications and frameworks.

TO LEARN MORE ABOUT TIA SUPPLY CHAIN SECURITY STANDARD, CONTACT US AT: SUPPLYCHAINSECURITY@TIAONLINE.ORG

FOOTNOTES

[1] ISO 27001 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.

[2] Requirement counts are considered to the lowest level of specificity. As an example, one requirement in SCS 9001 would be detailed as 8.4.4-s-1. Another requirement is 7.3.1-a. Another one is simply 7.1.1.

[3] For brevity, the SCS 9001 equivalent is limited to the specific control identifier, or the requirement to the x.y.z level of specificity. Future versions of this document may increase the granularity of the mapping.

[4] SCS 9001 defines requirements for a robust and documented Event and Incident Management Process including the need and how to report events and incidents to … designated officials and/or authorities (both internal and external). This requirement can be more explicit and is under consideration for enhancement in the next release of the standard.

[5] SCS 9001 is a comprehensive standard. Capabilities listed are in support of Supply Chain Security; there may be similar controls in ISO 27001, but they are centered on Information Security and are not process-based.

REFERENCES

ISO 27001 – available for purchase at ISO/IEC 27001:2022 – Information security management systems — Requirements

ISO 27002 – available for purchase at ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls

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

Other information and collateral regarding TIA's SCS 9001 Standard: TIA Supply Chain Security Program | TIA Online

United States National Cybersecurity Strategy (2023) available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-CybersecurityStrategy-2023.pdf