SCS 9001: Why ICT Security Must Go Beyond ISO 27001

The introduction of new technologies and fragmentation of the ICT network supply chain have enabled networks to become more efficient and software driven. While this shift is, in many ways, great for innovation, it also makes the supply chain more complex and vulnerable to threats.

The best way to ensure these vast supply chains are secure is through a comprehensive and certifiable global industry standard.

While the effort to bring SCS 9001—the world's first ICT-specific supply chain security standard—has been unprecedented, TIA didn't start from scratch. To date, TIA has managed the development of more than 3,600 ICT industry technical standards created by our member companies and their volunteers who have the necessary experience to streamline the normally rigorous process of developing new standards.

To that end, in building SCS 9001, the working group leading the effort reviewed the existing standards, security related architectures, models, and best practice documents that have been developed for security and supply chain management. One of note, ISO 27001, is the most widely deployed ISMS standard and has several excellent requirements and controls for securing organization's networks. Where appropriate, our team has utilized those concepts and customized them to support the demanding needs of ICT. In order not to recreate the wheel, the experts in the work group also used the other existing material as input for SCS 9001 and then added ICT-specific controls and measurements in order to ensure relevance and value for global technology buyers and suppliers.

One major difference between SCS 9001 and ISO 27001 comes with SCS 9001's detailed supply chain security measurements and benchmarking. In addition to the requirements and controls that an organization must implement to achieve certification, they must also submit quarterly supply chain security performance measurements into TIA's secure repository. The data is then aggregated and reported out anonymously. That is, for each specific measurement, trend data is shown for the industry average, best and worst in class performance. This same concept, understanding the industry performance without identifying individual company results, has been used by TIA's TL 9000 Quality Management System for over 20 years to drive continual improvement. SCS 9001 will do the same.

There are several other areas, such as zero trust architecture, software traceability, counterfeiting, supply chain management, and cloud controls, where SCS 9001 adds security requirements beyond what is in ISO 27001.

For more information on the differences between ISO 27001 and SCS 9001, the chart that follows compares each topic within the two standards and underscores why SCS 9001 will address a critical gap to help protect our global ICT supply chains.

Topic	ISO 27001	SCS 9001
Assets	Covers information assets	Covers information assets, cyber assets, manufacturing assets, design assets and network assets
Asset Classification	Yes	Yes
Risk Assessment	Requires repeatable method	Requires a three-factor risk assessment for all assets. Utilizing likelihood, impact, and control to calculate risk.
Residual Risk Assessment	Yes	Yes, but requires management signoff should identified risks exceed a defined risk appetite
Controls	114 controls in 18 domains that all must be applied	55 controls in 10 domains, only applied to reduce risk. Several other controls (which could be selectively applied) converted to process requirements which must be systematically implemented
Secure DLC	Weak	Very significant requirements added to ensure secure development of product throughout the lifecycle from concept to retirement
ID and Traceability	No	sBOM, and provenance requirements ensure trackability of SW & HW
Process Based	No, and ISO 27001 does not adequately (if at all) cover the issues addressed in the 7 SCS 9001 processes	Beyond the process implementation required to fulfill Quality Management System requirements for (ISO 9001, TL 9000, etc.), SCS 9001 requires the implementation of 7 processes to better control security within a company. (Technical Vulnerability management, Counterfeit Parts, Risk assessment and mitigation, HW, SW, Component Provenance, Secure SW/HW development, and Software Usage
Zero Trust Architecture	No	A Zero Trust Architecture plan is included the SCS 9001 requirements, understanding a full ZTA is not realistic to be fully implemented at day 1. Tracking progress against the plan is also required.
Business Continuity	Yes, but only with respect to ensuring information security during and security event. No testing is explicitly required	Requires the creation of business impact analysis, BC planning and BC Testing
Trust Principles	No	Yes, with full transparency of status against each Trust Principle
Underlying QMS	Not Required	Required. The underlying QMS must utilize Annex SL as used in ISO 9001, TL 9000, and other sector QMS's.
CMDB	Implied	Defined and required
Supply Chain Controls	Weak	Stronger and embedded in a supply chain process
Cloud Controls	Not included in ISO 27001, need ISO 27017, which may not be sufficient	Included though partnership with CSA
Measurements	None	Specifically defined and published in Annex B. All registered organizations must submit their results against these measurements to a secure repository utilizing similar processes and controls as for TL 9000
Benchmarking	None	Published quarterly to drive continual improvement
Certification Scheme	Yes	Yes
Assessor Competence	Loosely defined but required	Strongly defined and required

Questions about SCS 9001?
Send an email to supplychainsecurity@tiaonline.org

Telecommunications Industry Association