TIA QuEST Forum
Telecommunications Industry Association
TECHNICAL BULLETIN
TIAonline.org / @TIAonline

How SCS 9001 Supply Chain Security Standard Operationalizes the National Cyber Security Centre's 10 Steps to Cyber Security

April 21, 2022

Executive Summary

Government agencies, trade and standards organizations along with private industry are developing proposals in response to increasing cybersecurity threats. A new and impactful series of attacks have been experienced targeting the supply chain of vendors developing products for the ICT industry.

This bulletin provides an introduction to an initiative from the United Kingdom's National Cyber Security Centre (NCSC), the NCSC's 10 Steps to Cyber Security, and how the SCS 9001 Supply Chain Security standard from the Telecommunications Industry Association helps in achieving it's recommendations.

Introduction to the National Cyber Security Centre

Ofcom is the UK's communications regulator. Ofcom maintains a working relationship with NCSC, who provides technical advice on cyber security matters to support Ofcom in the exercise of its functions.

The NCSC was established in 2016 and is headquartered in London. It is the UK's technical authority on cyber security and advises the Secretary of State on national security matters relating to telecoms.

The organization has assembled expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure.

The NCSC provides security guidance for individuals, businesses, service providers, government agencies and cyber security professionals in the U.K. When cyber security attacks occur, the NCSC provides incident response support to help minimize impacts to the U.K.

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 solutions, TIA and its members are accelerating global connectivity across every industry and market. TIA is accredited by the American National Standards Institute (ANSI).

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 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 NCSC's 10 Steps to Cyber Security

The NCSC published its "10 Steps to Cyber Security" in May 2021.

This guidance aims to help organizations manage their cyber security risks by breaking down the task of protecting the organization into 10 Steps. Adopting security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring and minimizes the impact to the organization when incidents do occur.

The 10 Steps are:

- **Risk management:** take a risk-based approach to securing your data and systems.
- **Engagement and training:** collaboratively build security that works for people in your organization.
- **Asset management:** know what data and systems you have and what business need they support.
- **Architecture and configuration:** design, build, maintain and manage systems securely.
- **Vulnerability management:** keep your systems protected throughout their lifecycle
- Identity and access management: control who and what can access your systems and data.
- **Data security:** protect data where it is vulnerable.
- **Logging and monitoring:** design your systems to be able to detect and investigate incidents.
- **Incident management:** plan your response to cyber incidents in advance.
- **Supply chain security:** collaborate with your suppliers and partners.

How SCS 9001 Helps to Achieve the Goals of NCSC's 10 Steps to Cyber Security

The following table provides an overview of specific requirements and provisions within SCS 9001 that supports the goals of the NCSC 10 Steps to Cyber Security.

The provided examples are illustrative of the alignment and not necessarily all inclusive.

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 1 - Risk management: take a risk-based approach to securing your data and systems. This Step encourages organizations to consider how to approach and manage cyber risk. More details are available at: Risk management - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Top management drives security policies through-out the organization • Assessment of risk is performed at least annually • Ensuring that managers define security plans and measure the effectiveness of those plans at least annually • Development and retention of documentation for the security risk assessment process • Establishment of a Business Impact Analysis. • Establishment of a Business Continuity Plan. • Definition of specific controls to be implemented, along with measurements for performance benchmarking • Providing security awareness training • Deployment and operation of a secure network infrastructure. • Development of processes for detecting critical problems and how customers are notified of such problems

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 2 - Engagement and training: collaboratively build security that works for people in your organization. This Step provides recommendations for engaging with the work force and providing training in support of security policies. More details are available at: [Engagement and training - NCSC.GOV.UK]()	SCS 9001 supports this Step by requiring: • Managers in each functional area are responsible for implementing their security process and regularly assessing effectiveness. • Establishment of security awareness training for the entire organization including all employees, contractors, and 3rd parties who access the organization's IT assets, covering topics such as reporting security events, participating in security breach resolution, and understanding of the security controls and processes applicable to their area of control. • Maintenance of documented information for handling of identified critical problems and customer notification.
Step 3 - Asset management: know what data and systems you have and what business need they support. This Step emphasizes that organizations must have a detailed understanding of the assets operating within their environments to effectively manage in meeting security goals. More details are available at: [Asset management - NCSC.GOV.UK]()	SCS 9001 supports this Step by requiring: • The development of a complete asset inventory, including owner, patch levels, access rights, and location, as examples • That organizations establish sufficient policies for the disposal of assets at end of life and removal of sensitive data • The development of an Acceptable Use of Assets and Access Control policies • The creation of a mobile device policy, not limited to mobile phones • Establishment of cryptographic control policies for all assets • Equipment moved off-site for maintenance or repair are sanitized • Establishment of extensive auditing and logging capabilities to create a history of asset access.

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 4 - Architecture and configuration: design, build, maintain and manage systems securely. This Step advises organizations to consider security requirements from the outset within all business operations as the cyber security landscape is under constant change. More details are available at: Architecture and configuration - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Establishment of a plan for implementation of a Zero Trust Architecture. • Utilizing multi-factor authentication for access to systems. • Ensuring data is encrypted, both in transit and at rest. • Separation of production and non-production environments.
Step 5 - Vulnerability management: keep systems protected throughout their lifecycle. This Step provides recommendations in managing an organization's IT assets by managing vulnerabilities through the complete lifecycle of those assets. More details are available at: Vulnerability management - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Creation of a Technical Vulnerability Management processes to identify, evaluate, treat and report on security vulnerabilities • Secure Network and Systems Planning including system hardening, and monitoring • Secure Wireless Network Procedures • A plan for effective and consistent system patching • Use of vulnerability scanning tools. • Performing regular security testing including penetration testing • Establishing baseline security requirements for every IT asset
Step 6 - Identity and access management: control who and what can access your systems and data. This Step provides recommendations for controlling who and what can access your systems and data covering topics such as use of multi-factor authentication, Single-Sign On (SSO), and password policies, as examples. Further, this Step encourages the monitoring and creation of auditable logs to determine who has accessed what systems, when and for what reason. More details are available at: Identity and access management - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Having a formal Access Control Policy to ensure identity, entitlement, and access management for all corporate assets. • Using a Least Privilege Policy where all users are given the minimum privileges necessary to perform their function. • Deploying modern access control techniques such as SSO and multi-factor authentication. • Instituting an effective password policy covering all users accessing organizational assets including the removal of credentials when the need no longer exists. • Monitoring all access attempts, logging such activity and retaining those logs. • Authentication of APIs when using machine-to-machine communications.

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 7 - Data security: protect data where it is vulnerable. This Step emphasizes that Data be protected from unauthorized access, modification, or deletion. More details are available at: Data security - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • A Security Risk Analysis is performed and updated at least annually with organizations having an awareness of where sensitive data is stored and transmitted across networks. • Establishing a Media Management Policy which covers treatment of removal media, amongst other things. • Data is encrypted at rest and while in transit and cryptographic control policies are defined. • Systems are sanitized (sensitive data is removed) when reaching end of life or when removed from an organization's control such as when an asset is sent out for repair. • Data is backed up and archived. • Malware protections are in place. • An organization has policies to address data handling upon the expiration of business relationships with 3rd parties. • Data is segmented in multi-tenant architectures.
Step 8 - Logging and monitoring: design your systems to be able to detect and investigate incidents. This Step promotes developing an understanding of how assets are used and that logging and monitoring be foundations of security. More details are available at: Logging and monitoring - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Monitoring of infrastructure for anomalous traffic patterns and system access • Organizations monitor, control and enforce organizational communications for early detection of cyberattacks • Monitoring & controlling remote access • Extensive logging should be deployed including Event or operations logs, System Administrator logs, Logical access logs, Physical access logs, and Audit logs • Log files be protected against tampering • Alerts in the case of logging process failures • Assurance be provided for the protection, retention, and lifecycle management of audit logs, adhering to applicable legal obligations • As part of security monitoring, perform security testing with periodic penetration testing, a cyber-attack simulation, monitoring for specific threats, identification of dependencies and prioritization of vulnerabilities, and ensure appropriate testing.

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 9 - Incident management: plan your response to cyber incidents in advance. This Step encourages having a formal Incident Management plan to reduce the impacts to cost, productivity and reputation when cyber-attacks are experienced. More details are available at: Incident management - NCSC.GOV.UK	SCS 9001 supports this Step by requiring: • Organizations must establish an Incident Management Plan to restore services as quickly as possible and minimize the adverse impact on the business operations of the organization and its customers. • Update plans based on lessons learned as part of continuous improvement goals. • Examples of topics that the Incident Management Plan must address include: ○ definition of security incidents ○ defined roles and responsibilities ○ methods for reporting of incidents ○ the incident management process flow from detection and logging, categorization, and prioritization, diagnosing and investigation, resolution, closure, and post-incident evaluation for lessons learned ○ communicating with customers ○ incident classification and severity ratings ○ implementation of a security information and event management system or its equivalent, to aggregate relevant data from multiple sources ○ establishment and implementation of technical, organizational, and operational mechanisms to support the security incident management process ○ testing of the security incident response capability at least annually ○ analysis of the security impact of changes prior to implementation

NCSC 10 Steps to Cyber Security	TIA QuEST Forum SCS 9001
Step 10 - Supply chain security: collaborate with your suppliers and partners. This Step emphasizes that an attack on your suppliers can be just as damaging as one that directly targets the organization and suggests steps to take to encourage continuous improvement across your supply chain More details are available at: Supply chain security - NCSC.GOV.UK	SCS 9001 was created to address the problem of Supply Chain Security and that the security and supply chain management needs of the ICT industry are met. SCS 9001 supports this Step by requiring: • SCS 9001 requires that network operators and vendors deploy best practices for securing their business operations and ensuring the integrity of their products and services. • Organizations adopt a Supply Chain security risk assessment plan • Organizations adopt a Supply Chain security risk mitigation plan • Supply chain traceability is implemented to ensure the provenance of all assets are understood. • Specific measurements are implemented to define and monitor the minimum set of performance measurements.

References

The following references were used in the creation of this bulletin:

- How Ofcom and NCSC work together: Joint statement from Ofcom and the National Cyber Security... - NCSC.GOV.UK
- 10 Steps to Cyber Security - NCSC.GOV.UK
- UK TELECOMS SUPPLY CHAIN REVIEW REPORT: UK Telecoms Supply Chain Review Report (publishing.service.gov.uk)
- UK Telecom Securities Act: Telecommunications (Security) Act 2021 (legislation.gov.uk)
- NCSC-Vendor-Security-Assessment.pdf
- Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)

Questions? Want to get involved or learn more about SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

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.