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

How TIA QuEST Forum's SCS 9001 Supply Chain Security Standard Compares to the National Cyber Security Center's Cyber Essentials and Cyber Essentials Plus

June 09, 2022

Executive Summary

In 2014, the UK government developed a set of security guidelines known as "Cyber Essentials"[1]. Cyber Essentials defines a basic set of cyber security best practices that organizations should implement to protect themselves from cyber-attacks. Cyber Essentials is described as "*the minimum standard for cyber security in the UK*" and certification is required to do business with certain UK government agencies.

Cyber Essentials Plus is identical to Cyber Essentials, with the only difference being that Cyber Essentials is a self-certification and Cyber Essential Plus requires a third-party assessment. Within this bulletin, reference to Cyber Essentials will be used. This Technical Bulletin provides an overview of NCSC's Cyber Essentials and how the Telecommunications Industry Associate (TIA) QuEST Forum's SCS 9001 Supply Chain Security Standard accounts for the requirements and recommendations stated therein.

[1] The U.S. Federal Agency Cybersecurity and Infrastructure Security Agency, or CISA, has also produced a guide called CISA's Cyber Essentials. CISA's Cyber Essentials is targeted at small businesses and local government agencies to assist in developing an actionable understanding of where to start implementing organizational cybersecurity practices. These two initiatives are not to be confused; they are different.

Introduction to the National Cyber Security Centre (NCSC)

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

The NCSC has developed 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 in the U.K.

NCSC is the author of and maintains Cyber Essentials. Links to relevant information is available in the References section of this bulletin.

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.

Overview of Cyber Essentials

An Applicant for Cyber Essentials must ensure that their organization defines the boundary scope of certification and that the organization meets all the requirements. Evidence may be demanded from auditors conducting a Cyber Essentials Plus certification.

Cyber Essentials defines five technical control requirements:

1. Firewalls
2. Secure configuration
3. User access control
4. Malware protection
5. Security update management

An update to Cyber Essentials was announced in November 2021 and was published in January 2022. It is the most significant revision of the requirements since the original publication. Enhancements and clarifications have been made in response to new threats within a changing technology landscape. The new document is titled "Cyber Essentials: Requirements for IT infrastructure" and a link to it is available in the References section of this Technical Bulletin.

The primary enhancements focus on:

1. Cloud services: a set of shared responsibilities are defined for both the cloud provider and the cloud user. The five technical controls are mapped to the three main types of cloud services (IaaS, PaaS, SaaS).
2. Home working: addresses pervasiveness of remote workers that are now common, and in part driven and a result of the pandemic.
3. Passwords and multi-factor authentication: multi-factor authentication (MFA) provides additional protection, is widely available, and its use is encouraged.

Overview of Cyber Essentials Plus

Cyber Essentials and Cyber Essentials Plus are two different levels of certification. Cyber Essentials Plus has the same set of requirements as Cyber Essentials. Organizations will first be required to perform a self-assessment, with an independent certifying body responsible for verifying the answers. The Certification Body will then evaluate and test the organization's security practices.

Large organizations are expected to achieve Cyber Essentials Plus certification if employees have remote access to the corporate network.

NCSC has partnered with IASME as the assured service provider to oversee certifications to Cyber Essentials Plus. IASME works alongside a network of nearly 300 Certification Bodies across the UK and Crown Dependencies who are trained and licensed to perform Cyber Essentials Plus audits and to help organizations of all sizes in both cyber security and counter fraud prevention measures.

How SCS 9001 Aligns with NCSC's Cyber Essentials / Cyber Essentials Plus

The following table explains how SCS 9001 operationalizes the requirements and recommendations of Cyber Essentials.

Cyber Essentials Technical Requirements	TIA QuEST Forum SCS 9001 Alignment
Firewalls All internet connections must be secured by setting up network boundary firewalls to prevent unauthorized access and implement personal firewalls on PCs and other remote devices.	SCS 9001 defines extensive requirements for limiting access to network devices and services through the establishment of Access Control Policies for ensuring appropriate identity, entitlement, and access management for all corporate assets as well as a Workplace Policy which in part defines rules for home office / remote offices and mobile security. Firewall are included within these requirements, but the obligations go further with organizations expected to actively monitor networks and apply defense-in-depth techniques such as deep packet analysis, traffic throttling, and black-holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns to protect against a variety of attacks including distributed denial-of-service (DDoS) attacks.

Cyber Essentials Technical Requirements	TIA QuEST Forum SCS 9001 Alignment
Secure Configuration Devices must be secured by changing default settings and using passwords.	SCS 9001 requires numerous account protections such as multi-factor authentication, minimum password complexities, using a password generator, resetting default passwords, and account credential lifecycle management from instantiation through revocation. Additionally, SCS 9001 requires that passwords be protected both during storage and transmission with strong cryptographic controls employing a NIST Federal Information Processing Standards-valid cryptography standard (or equivalent) when used to protect the confidentiality of assets.
User Access Control Define user roles and permissions and configure access accordingly.	SCS 9001 requires that organizations have strict Asset Management, Asset Control, Workspace and Acceptable Use of Assets policies. Organizations must ensure appropriate identity, entitlement, and access management for all users and all corporate assets. SCS 9001 requires that organizations deeply instrument their operations in areas such as monitoring asset access, creating logs of administrative actions, network traffic, and automated equipment identification be used as a method of connection authentication, amongst other requirements.
Malware Protection Protect devices from malware, viruses and malicious attacks with the installation of the latest versions of anti-virus and anti-malware software and keep them up to date.	SCS 9001 requires that all devices have current anti-malware / anti-virus software installed. Additionally, SCS 9001 requires hardening of the corporate network and all end devices through Secure Network and Systems Planning. Finally, SCS 9001 requires annual Security Awareness Training for all employees, contractors, and 3rd party users with access to corporate assets. All individuals with access to organizational assets receive job-function level security awareness training organizational documented procedures, processes, and policies relating to their function.

Cyber Essentials Technical Requirements	TIA QuEST Forum SCS 9001 Alignment
Security Update Management Install software updates regularly to benefit by the most current security patches.	SCS 9001 requires a comprehensive asset inventory database be created and maintained. Within this database, all assets are recorded including hardware/software/firmware versions, software and patch levels. SCS 9001 also has explicit requirements for remote / mobile devices to ensure remote software updates and management is possible. Additionally, SCS 9001 has a requirement for measuring and reporting the timeliness of software updates as a reportable benchmark.
Back Up Your Data While not one of the 5 technical requirements, the most recent release of Cyber Essentials provides additional guidance in establishing a data backup strategy.	SCS 9001 requires that organizations create backup copies of all information, software and system images and that the process for backing up and restoring data is tested regularly. establish a Business Continuity Plan which includes the need for backing up and recovering data.
Cyber Essentials Scope While not one of the 5 technical requirements, the most recent release of Cyber Essentials provides coverage for the definition of 'in-scope' corporate assets. Recommendations are provided for: 1. Bring Your Own Device 2. Home working 3. Wireless devices 4. Externally managed services (cloud)	SCS 9001 is comprehensive in providing extensive coverage and flexibility in support for teleworkers using personal devices and operating over wireless infrastructures. 1. SCS 9001 defines BYOD Control Policies which the organization must establish, document and review annually for effectiveness. Examples of requirements within this policy include assessment of eligibility requirements, inventory of all such devices, requirements for backups of corporate data, maintenance and updates and the ability to remotely wipe as needed. 2. SCS 9001 requires establishment of a Workspace Policy which defines requirements for working from a home office or remote office as well as while being mobile. 3. SCS 9001 requires that the organization develop and implement processes and technical measures to protect wireless network environments. 4. SCS 9001 requires that organizations define a list of all approved cloud-based services and applications permissible. SCS 9001 requirements extend beyond the physical perimeter of the enterprise network and must be extended to cloud services and contractor networks, as examples.

Contrast of Cyber Essentials / Cyber Essentials Plus vs. SCS 9001

Cyber Essentials defines requirements for a basic level of security for organizations operating a network. SCS 9001 is a certifiable standard, as is Cyber Essentials Plus.

SCS 9001 is a much more comprehensive standard than Cyber Essentials.

Of special importance, is that SCS 9001 is a Supply Chain security standard and is intended to ensure the proper operational hygiene of all vendors in delivering products and services to organizations who operate networks, be they private or public.

SCS 9001 was developed in support of network operators in evaluating their vendors and providing higher assurance that vendors:

- Operate their businesses with integrity and transparency
- Conduct all aspects of operations and product development with a high level of security
- Deliver products that are inherently higher in security and quality
- 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.

Cyber Essentials Plus is a small subset of the protection provided by SCS 9001.

Questions? Want more information about TIA QuEST Forum's SCS 9001?
Visit: https://bit.ly/SCS9001
Send us an email: supplychainsecurity@tiaonline.org

References

Overview of Cyber Essentials:

About Cyber Essentials - NCSC.GOV.UK

Cyber Essentials: Requirements for IT infrastructure:

Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf (ncsc.gov.uk)

Differences between Cyber Essentials and Cyber Essentials Plus

The Main Differences-Cyber essentials vs Cyber Essentials PLUS (thetechblock.com)

The Difference Between Cyber Essentials and Cyber Essentials Plus (cybertecsecurity.com)

IASME Consortium Cyber Essentials Readiness Toolkit

Readiness | (iasme.co.uk)