A Guide to Contemporary Cybersecurity and Supply Chain Security Publications

TIA Industry Report

Version 0.2

Revision History

Version	Date	Comments
0.1	August 6, 2025	First draft
0.2	September 15, 2025	Second draft

Contents

Introduction

Cybersecurity and supply chain security are crucial practices that incorporate several strategies to protect digital assets, networks, and data from unauthorized access and cyber threats. While numerous industry standards development organizations, trade associations, global governments, and academia publish a wide range of standards, recommendations, and frameworks to address these threats, the sheer volume and diversity of these publications can create confusion. Organizations are often left feeling unsure about which publications are relevant to their business and how to use them to develop a truly effective and comprehensive security management system.

The Telecommunications Industry Association (TIA) developed this report to help organizations navigate the variety of cybersecurity and supply chain security publications. It provides an overview of the various entities that produce these publications, including their mission, focus, and key initiatives. This report also summarizes prominent publications and compares each to the TIA's own SCS 9001 Cybersecurity and Supply Chain Security standard. No single publication can address every security vulnerability, but combining specific publications outlined in this report can deliver more powerful outcomes than using any one publication alone.

The Telecommunications Industry Association (TIA)

TIA is the trusted industry association for the connected world, representing more than 400 global companies that enable high-speed communications networks and accelerate next-generation information and communications technology (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.

The TIA QuEST Forum brings together companies from around the world that manufacture, deploy, and operate cutting-edge networks to develop process-based industry standards and tools that improve business performance and address the challenges associated with digital transformation, new business models, innovation, and increasing competition. TIA's QuEST Forum community develops and maintains a prominent quality standard for the ICT industry—TL 9000.

As part of its commitment to ensuring global networks are reliable, trusted, and secure, TIA QuEST Forum released the SCS 9001 Supply Chain Security Management System. TIA SCS 9001 is the first comprehensive, measurable, and independently certifiable process-based supply chain security standard for the global ICT industry. It benchmarks performance to drive continuous improvement, providing value to network operators, developers, and manufacturers.

A Fragmented Industry Approach

In today's digital age, bad actors are launching attacks of all types across modern networks and the devices that comprise them. Unfortunately, consideration of security is too often compartmentalized, with many publications focusing narrowly on specific areas, such as:

- **Application Security**: Protecting specific software applications
- **Cloud Security**: Securing cloud infrastructure
- **Communications Security**: Safeguarding data in transit
- **Computer Security**: Protecting computing systems
- **Cybersecurity**: Defending against internet-based attacks
- **Endpoint Security**: Securing connected devices like mobile phones, laptops, and IoT devices
- **Information Security**: Protecting personal information, confidential business data, intellectual property, and other sensitive data from unauthorized access
- **Network Security**: Protecting network assets like servers
- **Operational Security**: Processes for security administering assets
- **Physical Security**: Protecting physical infrastructure and facilities from unauthorized access
- **Supply Chain Security**: Protecting the software, hardware, and other components that make up the vast and complex ICT supply chain

Each of these disciplines plays a pivotal role in forming a comprehensive defense strategy against the ever-evolving threat landscape. It is the position of TIA that to achieve material improvements to cybersecurity, all elements of security must be considered—because we are only as strong as our weakest link.

More Information

This report is designed to help organizations understand the variety of cybersecurity and supply chain security standards currently available. It's important to note that it is not intended to provide detailed mapping between standards; individual Technical Bulletins will be developed for further study based on user demand.

TIA selected the specific standards outlined in this report based on the interest expressed by its members, and we will continue to expand this document as needed. If you are interested in a review of a publication not included in this report, please contact TIA at questforum@tiaonline.org.

An Overview of Organizations Covered Within This Document

The numerous organizations that develop security publications are incredibly diverse. They include standards organizations, industry associations, government agencies, and others. This section provides a brief overview of the leading organizations whose works are featured in this document. While some of these organizations have a broad focus, this report concentrates on their cybersecurity and supply chain security initiatives.

Note that some standards are co-developed by multiple organizations, such as those from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). This collaboration is common for the following reasons:

- **Joint Technical Committees (JTCs)**: Organizations like ISO and IEC have established JTCs (e.g., ISO/IEC JTC 1 for Information Technology) to bring together experts from both organizations, ensuring the development of standards that address the needs of both the mechanical and electrotechnical sectors.
- **Harmonization of Standards**: By working together, standards organizations can create harmonized standards that are recognized globally. This promotes compatibility and interoperability of products and systems across different industries and regions.
- **Efficiency and Expertise**: By combining expertise, organizations can use resources more efficiently and create more comprehensive, higher-quality standards. For example, ISO/IEC standards leverage the strengths of ISO's broad industry reach and IEC's specialized knowledge in electrotechnology.
- **Global Consensus**: Jointly developed standards represent a worldwide consensus on best practices and technical specifications, which facilitates international trade and ensures that products meet the highest safety and performance standards.

Alliance for Telecommunications Industry Solutions (ATIS)

The Alliance for Telecommunications Industry Solutions (ATIS) is a leading technology and solutions development organization. It brings together nearly 200 global ICT companies to address key industry priorities such as 5G, network functions virtualization, cybersecurity, big data analytics, cloud services, and more. ATIS is accredited by the American National Standards Institute (ANSI) and is a North American Organizational Partner for the 3rd Generation Partnership Project (3GPP).

Organization URL: www.atis.org

Mission: ATIS aims to advance the ICT industry by developing innovative solutions and standards that drive the future of communications. Their vision is to be the premier organization for enabling the transformation of the ICT ecosystem.

Membership: ATIS includes a diverse membership of companies from across the ICT industry, including service providers, equipment manufacturers, software developers, and other stakeholders.

Key Initiatives:

- Mobile communications: Developing standards and solutions that will shape the future of 5G and 6G mobile communications through the Next G Alliance (NGA).
- Smart cities: Developing frameworks and standards to support the deployment of smart city technologies.
- Cybersecurity: Developing cybersecurity initiatives to improve the security of ICT networks and services, addressing emerging threats and vulnerabilities.
- Artificial Intelligence: Examining how Generative AI opens a new era of efficiency across sectors with the potential to reinvent the industry.
- ORAN: Launching an initiative to define a common set of baseline capabilities to simplify the deployment of Open RAN technology.
- Other activities include quantum computing and the integration of satellite communications with terrestrial networks.

American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system.

Founded in 1918, ANSI works closely with stakeholders from industry and government to develop standards and conformance-based solutions to national and global priorities. Standards and technical regulations impact up to 93% of international trade, helping to increase efficiency, open markets, boost consumer confidence, and reduce costs.

Organization URL: www.ansi.org

Mission: To enhance the global competitiveness of U.S. businesses and improve the quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems. ANSI does not develop standards itself but provides a framework for fair standards development and quality conformity assessment systems.

Membership: ANSI represents the interests of more than 270,000 companies and organizations and 30 million professionals worldwide.

Key Initiatives:

- Increasing outreach to diverse areas of industry to communicate the value and impact of standards and drive active participation.
- Acting as the sole U.S. representative to ISO, and, through the U.S. National Committee (USNC), to the IEC.
- Fostering U.S. competitiveness by providing relevant resources and assisting members and stakeholders with international trade issues affecting their business.
- Establishing ongoing standards collaboratives and partnerships to address specific standardization needs.
- Bridging the gap between industry and government by enabling information exchange and access among standards developing organizations and public-sector leaders, agencies, and legislators.
- Providing recognition of standardization achievements through its annual Leadership and Service Awards program.

Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization dedicated to improving cybersecurity for individuals, businesses, and governments. CIS is known for its CIS Critical Security Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data. These standards continuously evolve through a global community of IT professionals.

Organization URL: www.cisecurity.org

Mission: CIS aims to make the connected world safer by developing and promoting best practices for cybersecurity. Their vision is to lead the global community in securing our ever-changing connected world. CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats. They encourage collaboration and innovation to stay ahead of emerging threats.

Membership: CIS has a large and diverse membership. It includes over 12,000 IT security experts who contribute to the development of the CIS Benchmarks. These members come from various sectors, including government agencies, the military, large corporations, and academic institutions.

Key Initiatives:

- Developing security control recommendations and supplementary programs and tools, including CIS SecureSuite, CIS Hardened Images, CIS Benchmarks, and CIS Endpoint Security Services.
- Curating ongoing warning and analysis of current cybersecurity, physical threats, and online activity through the ThreatWA threat intelligence subscription program.
- Providing cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities through the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Providing network vulnerability assessments and remediation support for organizations.

Cybersecurity and Infrastructure Security Agency (CISA)

Established in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) is a component of the United States Department of Homeland Security (DHS). It is responsible for enhancing the security, resilience, and reliability of the nation's cybersecurity and infrastructure. CISA works across all levels of government and with the private sector to coordinate cybersecurity programs, improve protections against cyber threats, and respond to incidents.

Organization URL: www.cisa.gov

Mission: CISA's mission is to enhance the security, resilience, and reliability of the nation's cybersecurity and infrastructure.

Membership: Not applicable. CISA is a government agency with approximately 3,100 employees.

Key Initiatives:

- Protecting federal networks and critical infrastructure from cyber threats, including coordinating cybersecurity programs with state and local governments and private sector partners.
- Safeguarding critical infrastructure sectors such as energy, transportation, and communications from physical and cyber threats.
- Improving public safety and emergency communications interoperability across various levels of government and international borders.
- Improving incident response by providing support and coordination during cybersecurity incidents, helping organizations recover and mitigate damage.

Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is a nonprofit organization dedicated to promoting best practices and research in cloud security. CSA is committed to awareness, practical implementation, and certification for the future of cloud and cybersecurity. The organization is known for its comprehensive research program, which collaborates with industry, higher education, and government globally.

Organization URL: www.cloudsecurityalliance.org

Mission: CSA aims to define and raise awareness of best practices to ensure a secure cloud computing environment. They harness the expertise of industry practitioners, associations, governments, and their members to offer cloud security-specific research, education, certification, events, and products.

Membership: CSA has over 90,000 individual members and more than 500 corporate members worldwide. It operates globally with offices, partnerships, member organizations, and chapters, ensuring that CSA experts are accessible worldwide. This extensive network includes cloud service providers, security experts, and industry leaders who collaborate on research, education, and certification programs to enhance cloud security.

Key Initiatives:

- Cloud Control Matrix (CCM): A comprehensive cybersecurity control framework specifically designed for cloud computing, providing a structured set of controls to help organizations assess and manage cloud security risks.
- CSA Security, Trust & Assurance Registry (STAR): A three-tiered provider assurance program of self-assessment, third-party audit, and continuous monitoring, leveraging the CCM.
- Certificate of Cloud Security Knowledge (CCSK): The industry's first cloud security user certification, setting the benchmark for professional competency in cloud computing security.
- Certified Cloud Security Professional (CCSP): Certification developed in collaboration with the International Information System Security Certification Consortium (ISC2), representing advanced skills required to secure the cloud.

Consumer Technology Association (CTA)

The Consumer Technology Association (CTA) is a trade association that represents the U.S. consumer technology industry, which is valued at around $505 billion and supports over 18 million jobs.

Organization URL: www.cta.tech

Mission: CTA aims to help innovators of all sizes grow their businesses and improve people's lives through technology.

Membership: CTA includes over 1,500 member companies, ranging from startups to multinational corporations.

Key Initiatives:

- Research and Standards: The association provides market research and develops industry standards to help guide the technology sector. Examples include CTA-2088, a standard that specifies baseline cybersecurity capabilities for devices and device systems, and CTA-2132, an IoT Product Cybersecurity Risk Assessment standard that provides a framework for conducting cybersecurity threat or risk assessments for IoT products.
- Cyber Labeling for Connected Devices: A public-private effort led by the White House, with input from CTA, the National Institute of Standards and Technology (NIST), and other stakeholders. This program aims to create a voluntary cybersecurity label for consumer IoT devices known as the U.S. Cyber Trust Mark program.
- Advocacy: CTA works on Capitol Hill to protect the innovation economy from restrictive laws and regulations.
- Events: CTA organizes events like the Consumer Electronics Show (CES), one of the world's largest tech trade shows.
- Consumer Technology Circularity Initiative (CTCI): An initiative that focuses on reducing waste, encouraging reuse, enhancing recycling, and minimizing the climate impact of consumer electronics.
- Sustainability Report: Highlights the tech industry's efforts to create a more sustainable future, including reducing energy consumption, promoting responsible recycling, and encouraging the use of renewable energy.

ENX Association

Founded in 2000, ENX Association is an organization consisting of automobile manufacturers, suppliers, and national automotive associations. With its association structure, ENX is the initiator and governing body of common standards and interoperable services based on these standards. ENX acts as a neutral governance and escalation authority as well as a driver of ongoing development for the users.

Organization URL: www.enx.com

Mission: The ENX Association aims to enable and simplify secure and trustworthy collaboration over industrial value-added networks.

Membership: The Association currently has 15 members, including Audi, BMW, Bosch, Continental, Daimler, Ford, Renault, and Volkswagen, as well as national automotive associations from Spain (ANFAC), France (GALIA), the UK (SMMT), and Germany (VDA).

Key Initiatives:

- ENX Network: This initiative provides a secure and standardized communication network for the automotive industry, enabling safe data exchange and collaboration among manufacturers, suppliers, and service providers
- Trusted Information Security Assessment Exchange (TISAX): This key industrial cybersecurity assessment program governed by the ENX Association ensures that companies meet high standards of information security, which is crucial for protecting sensitive data and maintaining trust within the industry/
- Digitalization and Industry 4.0: ENX supports the digital transformation of the automotive industry by developing standards and solutions that address the challenges of digitalization, such as cybersecurity, data protection, and interoperability
- Cyber resilience: the association works on enhancing the cyber resilience of the automotive industry by promoting multi-layered security measures and uninterrupted just-in-time production.

European Telecommunications Standards Institute (ETSI)

Established in 1988, the European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit organization funded by its members and the European Union. ETSI plays a crucial role in the development of globally applicable standards for ICT technologies. ETSI considers socioeconomic trends and policy initiatives, such as climate change, energy efficiency, and the UN's Sustainable Development Goals, in its strategic planning.

Organization URL: www.etsi.org

Mission: ETSI aims to produce high-quality standards that enable interoperability, security, and competitive advantage across various sectors of industry and society. Although initially focused on European needs, ETSI's standards are now used worldwide. They collaborate with international organizations to support global ICT standardization.

Membership: ETSI has over 850 member organizations from more than 60 countries, including companies, research bodies, and government agencies.

Key Initiatives:

- Standards development: ETSI is involved in developing standards for telecommunications, broadcasting, and other electronic communications networks and services. They also work on emerging technologies like 5G, Internet of Things (IoT), and cybersecurity.
- Digital transformation: ETSI is at the forefront of standardizing new and existing digital technologies, enabling comprehensive end-to-end ICT architectures and technologies, including devices, networks, and cloud.
- Innovation and market-driven standards: ETSI promotes innovation in ICT by developing standards that are timely, high-quality, and responsive to market needs. This includes areas like AI, machine learning, cloud computing, and quantum computing.

GSM Association (GSMA)

The GSM Association (GSMA) is a global trade organization representing mobile network operators, technology companies, and other stakeholders in the mobile industry. It was formed in 1995 as the GSM MoU (Memorandum of Understanding) Association to support and promote mobile operators using the GSM standard. It has since evolved to support a wide range of mobile technologies worldwide.

Organization URL: www.gsma.com

Mission: GSMA aims to unify the mobile industry and drive positive business environments and societal change through mobile technology.

Membership: GSMA includes nearly 800 mobile operators and almost 300 companies in the broader mobile ecosystem, such as handset and device makers, software companies, equipment providers, and internet companies.

Key Initiatives:

- MWC (Mobile World Congress): GSMA organizes the world's largest mobile industry events, including MWC Barcelona, MWC Shanghai, and MWC Los Angeles.
- Industry Programs: Major programs include initiatives like Future Networks, Identity, and the Internet of Things (IoT), which aim to promote standards and interoperability for new mobile technologies.
- Policy and advocacy: GSMA represents the mobile industry to governments and institutions, advocating for fair and flexible regulatory frameworks and the timely allocation of radio spectrum for mobile services.
- GSMA Open Gateway: This initiative focuses on unlocking the full potential of 5G networks by commercializing Application Programming Interfaces (APIs). More than 40 mobile operator networks across five continents have commercially launched network API services through this initiative.

International Electrotechnical Commission (IEC)

Founded in 1906, the International Electrotechnical Commission (IEC) is a global, non-governmental organization that develops and publishes international standards for all electrical, electronic, and related technologies. The IEC has a long history of facilitating global trade and innovation by creating standards that are recognized and used worldwide.

Organization URL: www.iec.ch

Mission: The IEC aims to promote international cooperation on all questions of standardization and related matters in the fields of electrotechnology. Their vision is to ensure that products and systems work safely and efficiently together.

Membership: The IEC comprises over 170 countries, with each member representing the IEC in their respective countries.

Key Initiatives:

- Standards development: The IEC has published over 10,000 international standards covering a wide range of technologies, from power generation and distribution to home appliances and office equipment.
- Education and outreach: The IEC provides educational resources to enhance the understanding of their standards and programs designed to increase participation at all levels of standardization.
- Global Impact Fund: The IEC partners with organizations to bring the value of their work to communities, such as e-waste efforts, providing reliable electricity to rural communities, and reducing emissions.

International Organization for Standardization (ISO)

Founded in 1947, the International Organization for Standardization (ISO) is an independent, non-governmental international organization that develops and publishes standards to ensure the quality, safety, efficiency, and interoperability of products, services, and systems. ISO has been instrumental in facilitating international trade and cooperation by creating standards that are recognized and used worldwide.

Organization URL: www.iso.org

Mission: ISO aims to bring together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges.

Membership: ISO comprises 172 national standards bodies, with each member representing ISO in its respective country. This ensures a broad and inclusive approach to standard development.

Key Initiatives:

- Standards development: ISO has published over 25,000 international standards covering almost all aspects of technology and manufacturing, from food safety and healthcare to information technology and environmental management.
- Public awareness and education: ISO works to raise public awareness of and promote the teaching of standards and standardization, including working with other standards organizations like IEC.

ioXt Alliance

The ioXt Alliance is a global organization dedicated to establishing security standards for IoT devices. It brings together manufacturers, industry alliances, and government organizations to harmonize best security practices and create testable standards. These standards aim to ensure that IoT products are secure, upgradable, and transparent, giving consumers and retailers confidence in their connected devices.

Organization URL: www.ioxtalliance.org

Mission: The ioXt Alliance focuses on addressing device vulnerabilities, such as passwords, network, Bluetooth, gateway, and cloud issues, through its certification program. By setting these standards, the alliance helps protect devices and maximize product reliability and compatibility.

Membership: The ioXT Alliance has over 580 active members that include a diverse range of industry-leading tech companies and global manufacturers committed to advancing IoT security standards.

Key Initiatives:

- Security standards: Establishes universal IoT security standards to address device vulnerabilities, such as passwords, network, Bluetooth, gateway, and cloud issues.
- Certification Program: Provides a certification program that ensures IoT products meet the established security standards, including testing and verifying compliance to maximize product reliability and compatibility.
- Public policy: Collaborates with industry partners to set responsible public policies that bring security, upgradability, and transparency to consumers.
- The ioXT Security Pledge: Outlines key security principles, such as no universal passwords, secured interfaces, proven cryptography, security by default, verified software, automatic security updates, vulnerability reporting programs, and transparency about security update periods.
- Partnerships: working with organizations like PSA Certified to improve silicon security and ensure that connected products are protected from the silicon level through to end products and services.

MITRE Corporation

Founded in 1958, the MITRE Corporation (MITRE) was initially sponsored by the U.S. Air Force to bridge the gap between academic research and industry. Over the years, it has expanded its focus to include a wide range of areas such as cybersecurity, healthcare, aviation safety, and more. MITRE is a not-for-profit organization that operates federally funded research and development centers (FFRDCs) and works to solve problems for a safer world.

Organization URL: www.mitre.org

Mission: MITRE's mission is to advance national security and serve the public interest as an independent adviser. Their vision is to pioneer a better future by ensuring the safety and security of the nation. MITRE's focus areas include aerospace, artificial intelligence, cybersecurity, defense and intelligence, government innovation, health, homeland security, telecom, and transportation.

Membership: Not applicable. MITRE has over 9,000 employees.

Key Initiatives:

- Global impact: MITRE's work has a significant impact on national security, public safety, and technological advancement. They are involved in projects ranging from GPS and 5G/6G development to cancer research and autonomous vehicle technology.
- MITRE System of Trust (SoT): A comprehensive framework designed to assess and manage supply chain security risks, SoT provides a standardized methodology for evaluating the trustworthiness of suppliers, supplies, and service providers.
- MITRE ATT&CK Framework: A comprehensive knowledge base of cyber adversary tactics and techniques used to improve cybersecurity defenses.
- Common Vulnerabilities and Exposures (CVE): CVE is a standardized system for identifying and naming publicly known cybersecurity vulnerabilities.
- Common Weakness Enumeration (CWE): CWE is a comprehensive list of software and hardware weaknesses designed to help developers and security practitioners identify and address vulnerabilities in their systems.
- National Cybersecurity Federally Funded Research and Development Center (NCF): The NCF is sponsored by NIST and operated by MITRE as the country's only FFRDC dedicated solely to cybersecurity.

National Institute of Standards and Technology (NIST)

Founded in 1901, the National Institute of Standards and Technology (NIST) is a U.S. government agency established to address the need for a reliable measurement infrastructure to support U.S. industry. NIST plays a crucial role in promoting innovation and industrial competitiveness.

Organization URL: www.nist.gov

Mission: NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Membership: Not applicable. NIST is a government agency with approximately 3,400 employees.

Key Initiatives:

- Special publications (SPs): SPs are documents that provide guidelines, recommendations, and technical specifications on various topics, including cybersecurity, supply chain security, and information technology. Organizations use these publications to enhance their security practices and comply with regulatory requirements. Examples include NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-37 Risk Management Framework for Information Systems and Organizations, and NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.
- Cybersecurity Framework: NIST developed the Cybersecurity Framework to help organizations manage and reduce cybersecurity risks. This framework is widely used across various sectors.
- Smart grid: NIST is involved in developing standards and guidelines for the smart electric power grid, which aims to improve the efficiency and reliability of electricity distribution.
- Advanced manufacturing: NIST supports advanced manufacturing through research and the development of standards that enhance the competitiveness of U.S. manufacturers.
- Global impact: NIST's standards and research have a significant impact on global trade, technology development, and public safety. Their work ensures that products and services are safe, reliable, and of high quality.

Open Group

The Open Group is a global consortium that aims to enable the achievement of business objectives through the development of open, vendor-neutral technology standards and certifications. Their work supports a wide range of industries, including finance, healthcare, government, and telecommunications.

Organization URL: www.opengroup.org

Mission: The Open Group's mission is to drive the creation of Boundaryless Information Flow™ achieved by working with customers, suppliers, consortia, and other standards bodies. Their vision is to enable access to integrated information within and between enterprises based on open standards and global interoperability.

Membership: The Open Group includes a diverse membership of over 800 organizations, including businesses, government agencies, and academic institutions. Members collaborate to develop standards and certifications that address the needs of the global IT community.

Key Initiatives:

- The Open Trusted Technology Provider™ Standard (O-TTPS): This standard focuses on supply chain security and countering risks related to tainted and counterfeit components. O-TTPS serves as the foundation for the ISO/IEC 20243 international standard.
- The Open Group Architecture Framework (TOGAF®): A widely used framework for enterprise architecture that provides a comprehensive approach to designing, planning, implementing, and governing enterprise information architecture.
- ArchiMate®: An open and independent modeling language for enterprise architecture, providing instruments to support the description, analysis, and visualization of architecture within and across business domains.
- Open FAIR™: A standard for risk analysis and risk management, providing a model and taxonomy for understanding, analyzing, and measuring information risk.
- Standards development: The Open Group develops standards through a consensus-driven process, ensuring that they meet the needs of the global IT community and support interoperability and innovation.

SAE International (SAE)

Founded in 1905, SAE International, formerly known as The Society of Automotive Engineers (SAE), is a global association of engineers and related technical experts in the aerospace, automotive, and commercial-vehicle industries. SAE has a long history of developing standards and fostering innovation in the mobility sector. It was initially focused on the automotive industry but has since expanded to include aerospace and commercial vehicles. SAE is a non-profit organization.

Organization URL: www.sae.org

Mission: SAE aims to advance mobility knowledge and solutions for the benefit of humanity. Their vision is to be the leader in connecting and educating mobility professionals, enabling safe, clean, and accessible mobility solutions.

Membership: SAE has over 138,000 global members, comprising professionals and students from various sectors of the mobility industry, including automotive, aerospace, and commercial vehicles.

Key Initiatives:

- Standards development: SAE develops a range of standards to ensure the cybersecurity of connected vehicles, including ISO/SAE 21434, a standard focused on cybersecurity engineering for road vehicles and the SAE J2945/x and SAE J3161/x series, which ensure the authenticity and integrity of communications through digital signatures and certificates.
- Electric vehicle (EV) charging infrastructure: SAE is working on standardizing the North American Charging Standard (NACS) connector to ensure interoperability and reliability across EV charging stations. This includes developing a Public Key Infrastructure (PKI) for cyber-secure charging.
- Aerospace standards: SAE has been actively updating and publishing new aerospace standards, with over 500 aerospace and systems management standards released in 2023, including significant revisions to aviation safety documents and new guidelines for cybersecurity in propulsion systems.
- Sustainable mobility solutions: SAE's Sustainable Mobility Solutions arm focuses on initiatives that lead to net-zero transportation, including efforts to align industry and government actions to advance sustainable mobility on a national level.

Telecommunications Industry Association (TIA)

The Telecommunications Industry Association (TIA) is the trusted association for the connected world, representing more than 400 organizations that enable high-speed communication networks and accelerate next-generation technology innovation. As a member-driven organization, TIA advocates for the industry in the U.S. and internationally, develops critical standards, manages technology programs, and improves business performance.

Organization URL: www.TIAonline.org

Mission: TIA aims to enable high-speed networks and accelerate next-generation ICT innovation by being the trusted industry association for the connected world.

Membership: TIA has a global membership of more than 400 companies, including manufacturers, suppliers, network operators, service providers, distributors, and systems integrators operating within the ICT industry and associated verticals.

Key Initiatives:

- Standards development: TIA is accredited by the American National Standards Institute (ANSI) to develop industry standards for ICT products, such as cellular towers, data terminals, VoIP devices, and more.
- Policy and advocacy: TIA represents the ICT industry in policy discussions, advocating for regulations that promote innovation and investment in high-speed networks.
- Technology programs: TIA brings together member companies and other stakeholders across a variety of industries to facilitate technology-based communities of interest that convene to solve unique challenges, shape solutions, and provide strategic guidance to enable next-generation ICT products and services across markets.
- QuEST Forum: Formed in 1998 to address the challenges of digital transformation, new business models, innovation, and increasing global competition, QuEST Forum brings together companies from around the world 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. QuEST Form develops and maintains the TL 9000 Quality Management System, the ICT industry's most prominent quality standard, and the SCS 9001 Supply Chain Security Management Systems, the ICT industry's first comprehensive, measurable, and independently certifiable process-based supply chain security standard.

UL Solutions (UL)

UL Solutions, formerly known as Underwriters Laboratories (UL), is a global leader in safety science. Founded in 1894, UL started as a laboratory for testing electrical components and fire safety. Over the years, it has expanded its scope to include a wide range of safety, security, sustainability, and performance testing. UL operates in over 110 countries, supporting a wide range of industries including automotive, aerospace, consumer electronics, and healthcare.

Organization URL: www.ul.com

Mission: UL aims to make the world a safer, more secure, and sustainable place by advancing safety science and advocating for safe living and working environments. UL provides testing, inspection, and certification services. They also offer software and advisory services to support product innovation and business growth.

Membership: Not applicable. UL Solutions is a public company with over 15,000 employees.

Key Initiatives:

- Testing and certification: UL provides comprehensive testing, inspection, and certification services to ensure products meet regulatory and safety standards, including recognized UL certification marks that serve as symbols of trust to indicate that a product has been tested and meets UL's stringent safety standards.
- Research and standards development: UL develops standards for safety, security, and sustainability, which are used globally to ensure product reliability and safety.
- Sustainability and innovation: UL supports sustainable practices and helps companies innovate safely, from electrification to 5G and new mobility solutions.
- Advisory services: UL offers expert advisory services to help businesses navigate complex regulatory environments and improve their safety and sustainability practices.
- Software solutions: UL develops software tools to help companies manage compliance, enhance supply chain transparency, and operationalize sustainability.

United States Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)

The U.S. Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) oversees all Department of Defense (DoD) acquisitions, including procurement of goods and services, research and development, developmental testing, and contract administration. This includes managing the DoD Acquisition System, system design and development, production, logistics, and distribution.

The President appoints the Under Secretary of Defense for Acquisition and Sustainment with the consent of the Senate and serves as the principal staff assistant and advisor to the Secretary of Defense on all matters related to acquisition and sustainment.

Organization URL: www.acq.osd.mil

Mission: The primary mission is to enable the delivery and sustainment of secure and resilient capabilities to the warfighter and international partners in a timely and cost-effective manner.

Membership: Not applicable. The OUSD(A&S) is part of the larger Defense Acquisition Workforce, which includes nearly 186,000 civilian and military professionals from various departments and defense agencies.

Key Initiatives:

- The Cybersecurity Maturity Model Certification (CMMC): Developed through contracts with Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory, and Futures, Inc., the CMMC aims to enhance the cybersecurity posture of companies in the Defense Industrial Base (DIB) by ensuring they have adequate controls in place to protect sensitive information.
- Strategic goals: The office operates under the framework of the National Defense Strategy (NDS), focusing on restoring military readiness, expanding and strengthening alliances and partnerships, and bringing business reform to the DoD.
- Key areas include military construction, material readiness, maintenance, environment and energy resilience, and international cooperation.

Overview of Contemporary Security Publications

ANSI / CTA-2088

Snapshot

Publication Title:	Baseline Cybersecurity Standard for Devices and Device Systems
Publication Number:	ANSI/CTA-2088-A
Publication Type:	Standard
Primary Use Case:	Baseline operational security for connected consumer devices
Target Industry:	IoT
Current Version:	N/A
Date of Last Release:	May, 2022
Developing Organization(s):	Consumer Technology Association (CTA)
Certifiable? (Yes / No):	Yes
Where to get it:	Baseline Cybersecurity Standard for Devices and Device Systems (ANSI/C – Consumer Technology Association® (cta.tech)
Free? (Yes / No):	Yes

Overview

ANSI/CTA-2088 is a standard developed by the CTA that specifies baseline cybersecurity capabilities for devices and device systems. This standard addresses the ever-increasing amount and types of connected devices, from thermostats to fitness trackers, ovens, and smart TVs. It outlines a set of operational cybersecurity capabilities that any connected consumer device should possess. The standard encompasses not only the individual devices but also the components that make up these devices, such as hardware modules, chips, software, sensors, and other operating components.

CTA has expanded the original standard and has extended the requirements to address the unique cybersecurity needs of small Unmanned Aerial Systems (sUAS), ensuring that these systems are protected against potential cyber threats.

Comparison to TIA SCS 9001

ANSI/CTA-2088-A provides a baseline level of operational security and data protection for IoT devices. It is similar to peer standards like ETSI EN 303 645 and NIST IR 8425. The scope of

ANSI/CTA-2088-A is stated as specifying “baseline device security capabilities and related organizational security capabilities and recommendations for devices and device systems, including for individual connected devices, endpoint devices, components, hardware modules, chips, software, sensors, or other operating components.”

Accordingly, the standard provides a set of requirements for establishing baseline operational security for devices, as well as organizational requirements for the design and support of devices throughout their lifetime.

Examples of device requirements include:

- Encrypting data and cryptographic practices
- An ability to uniquely identify the device
- Password management
- Use of secure networking protocols
- Data validation
- Device must be in-field upgradeable to accept software security patches
- The ability to log events

Examples of organizational requirements include:

- The use of secure development practices
- Avoidance of common web application attack threats in device architecture
- Awareness of common threats introduced by the choice of programming languages
- Assessing vulnerabilities
- Notifications of product lifecycle and availability of security patches
- Device documentation

TIA SCS 9001 is network, technology, and product independent. It does not include specific requirements for securing specific product categories, such as consumer devices, but it does provide similar requirements. TIA SCS 9001 is used to certify an organization and its security practices to ensure that the supplier can be trusted.

TIA SCS 9001 and ANSI/CTA-2088-A can be used together to provide a more powerful outcome for IoT security than either standard by itself.

ATIS 5G Network Assured Supply Chain

Snapshot

Publication Title:	ATIS 5G Network Assured Supply Chain Standard
Publication Number:	ATIS-I-0000090
Publication Type:	Standard
Primary Use Case:	Supply Chain Security
Target Industry:	5G Mobile Networks
Current Version:	N/A
Date of Last Release:	June, 2022
Developing Organization(s):	Alliance for Telecommunications Industry Solutions (ATIS)
Certifiable? (Yes / No):	Yes
Where to get it:	ATIS Document Center (accuristech.com)
Free? (Yes / No):	No

Overview

The ATIS 5G Network Assured Supply Chain standard aims to ensure the security and reliability of 5G networks with a focus on supply chain requirements. It defines a set of controls and requirements that apply across the supply chain lifecycle, ensuring that hardware and software components adhere to the highest levels of assurance. The standard has a strict focus on 5G core networks and explicitly states it does not address mobile handsets or other terminal devices.

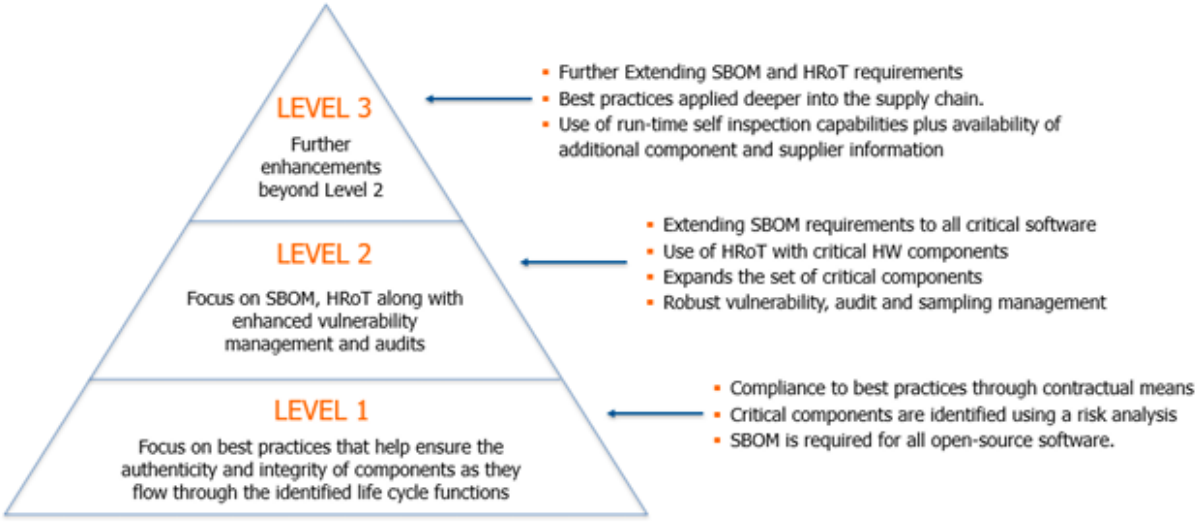
The ATIS 5G Supply Chain Working Group (5G/SC WG) leads this effort, focusing on Supply Chain Risk Management (SCRM) principles to ensure the integrity of 5G networks and the data they carry, while recognizing the evolving nature of threats and the need for continuous adaptation. The framework provides a multi-layered view of the 5G supply chain ecosystem, assessing threats and vulnerabilities at each stage of the lifecycle, from design to post-operation.

The first half of the standard introduces topics such as 5G network architecture, supply chain risks, and software bills of materials (SBOMs). A series of appendices covers future initiatives or provides additional supplemental information. Chapter 8 of the standard includes a total of 56 requirements organized into the following top-level categories:

- Software and Software-Controlled Hardware Requirements
- Secure Design Through Build

- Cybersecurity Hygiene in Post Build Supply Chain Lifecycle Functions
- Management and Administrative Requirements

The standard also accommodates three levels of supply chain assurance as identified in the following graphic.[1]



Comparison to TIA SCS 9001

ATIS-I-0000090 is a well-written standard that offers various levels of assurance, which can be implemented in a phased approach as required. It is intended to be used solely in the 5G industry.

TIA SCS 9001 is a more comprehensive standard covering a larger set of requirements to address supply chain security as applied to any ICT vertical. It does not offer different levels of certification, but does provide flexibility through the scope, Statement of Applicability (SoA), and other provisions. TIA SCS 9001 is essentially a superset of ATIS-I-0000090.

[1] Graphic is taken from ATIS-I-0000090

CIS Critical Security Controls

Snapshot

Publication Title:	CIS Critical Security Controls
Publication Number:	N/A
Publication Type:	Best Practice Recommendations
Primary Use Case:	A prioritized set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks.
Target Industry:	Any subjected to cyber attacks.
Current Version:	V8.1
Date of Last Release:	June 25, 2024
Developing Organization(s):	Center for Internet Security (CIS)
Certifiable? (Yes / No):	No
Where to get it:	CIS Controls (cisecurity.org)
Free? (Yes / No):	Yes

Overview

CIS Critical Security Controls are a set of best practices that offer a prioritized, prescriptive approach for organizations of all sizes to mitigate the risk of cyber-attacks that exploit weaknesses, such as unpatched software, poor configuration management, and outdated solutions. Developed through a consensus process involving a global community of cybersecurity experts, this comprehensive set of guidelines is structured around a set of safeguards that simplify the process of protecting against the most common cyber threats. Several U.S. states recognize the CIS Critical Security Controls as a standard for demonstrating compliance with state and federal cybersecurity regulations.

The latest version, v8.1, emphasizes adaptability to the evolving digital landscape, including the shift towards hybrid and cloud environments, and the need for security across the supply chain. CIS Critical Security Controls are divided into 18 categories, each addressing a specific aspect of cybersecurity, ranging from asset and software inventory management to incident response and penetration testing. They are organized into three Implementation Groups (IGs) that represent an increasing level of protection based on their implementation. In aggregate and across the 18 categories, CIS Critical Security Controls provide a total of 153 safeguards.

Comparison to TIA SCS 9001

CIS Critical Security Controls are a practical framework to improve cyber hygiene. It has been mapped to numerous government regulations and offers several levels of implementation, resulting in an enhanced security posture. It focuses on cybersecurity and provides little support for supply chain security. Further, it is not certifiable.

TIA SCS 9001 is a certifiable standard that addresses the challenges of ICT supply chain security. TIA SCS 9001 and CIS Critical Security Controls are mostly complementary. TIA SCS 9001 encompasses most of the CIS Critical Security Controls as process-based requirements, which establish expectations for establishing key performance indicators within critical processes to measure results and drive continuous improvement.

CISA Secure by Design

Snapshot

Publication Title:	Shifting The Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software
Publication Number:	N/A
Publication Type:	Guidance and best practices
Primary Use Case:	Development of secure software
Target Industry:	Software manufacturers and developers
Current Version:	N/A
Date of Last Release:	October 25, 2023
Developing Organization(s):	The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and several international partners.
Certifiable? (Yes / No):	No
Where to get it:	Secure By Design (cisa.gov)
Free? (Yes / No):	Yes

Overview

CISA's Secure by Design is a cybersecurity framework that emphasizes the importance of integrating security measures from the initial design and development phases of systems and infrastructure. This approach is proactive, aiming to embed security into the very fabric of technology, making it an inherent and inseparable aspect rather than an afterthought or a mere add-on. The principle behind Secure by Design is that software manufacturers should not wait for vulnerabilities to be exploited before taking action. Instead, they should anticipate potential security threats and mitigate them in advance by building products that are inherently resistant to attacks.

Secure by Design encourages manufacturers to prioritize the integration of product security as a prerequisite to features and speed to market. Similarly, the European Union reinforces the importance of product security in the Cyber Resilience Act, emphasizing that manufacturers should implement security throughout a product's life cycle to prevent them from introducing vulnerable products into the market.

Secure by Design also references and recommends the Secure Software Development Framework (SSDF), also known as the National Institute of Standards and Technology's (NIST's) SP 800-218. The SSDF is a core set of high-level secure software development practices that can

be integrated into each stage of the development lifecycle. Secure by Design is the result of contributions from many international government centers for cybersecurity.

Comparison to TIA SCS 9001

Both publications are intended to improve supply chain security. Secure by Design is a framework of best practices with a focus on improving secure software development practices to create a higher level of organizational accountability.

TIA SCS 9001 is a more comprehensive document that assesses additional organizational processes beyond the software development life cycle. Secure by Design and TIA SCS 9001 can be used together to create more powerful outcomes than implementing either publication by itself.

Cybersecurity Maturity Model Certification (CMMC)

Snapshot

Publication Title:	Cybersecurity Maturity Model Certification (CMMC)
Publication Number:	2.0
Publication Type:	Framework
Primary Use Case:	Enhanced cybersecurity for Defense Industrial Base (DIB)
Target Industry:	U.S. Department of Defense Contractors
Current Version:	2.0
Date of Last Release:	November, 2021
Developing Organization(s):	U.S. Department of Defense (DoD)
Certifiable? (Yes / No):	Yes
Where to get it:	About CMMC (defense.gov)
Free? (Yes / No):	Yes

Overview

CMMC is a comprehensive framework established by the DoD to enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC aims to ensure that DIB contractors implement robust cybersecurity standards to protect sensitive unclassified information.

The CMMC framework is characterized by its tiered model, which categorizes contractors based on the type and sensitivity of the information they handle. The three levels of the framework—Foundational, Advanced, and Expert—each include a set of practices and objectives tailored to the level of cybersecurity maturity expected.

- Level 1: Foundational cybersecurity practices, including 17 requirements
- Level 2: Advanced cybersecurity practices, including 110 requirements
- Level 3: Expert cybersecurity practices, including over 100 requirements.

The expectations of CMMC are organized as several practices and sub-practices that are individually assessed during a certification, including:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)

- Risk Assessment (RA)
- Security Assessment (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

The implementation of CMMC Version 2.0 is a phased process, with assessments beginning in the first quarter of 2025 and a gradual rollout in DoD contracts expected to start in the third quarter of the same year. This approach allows for a transition period for contractors to understand, prepare for, and meet the required cybersecurity standards. The CMMC Accreditation Body, under the oversight of the DoD CIO office, establishes, manages, controls, and administers the CCMC assessment, assessor certification, training, and accreditation process for the DoD supply chain.

Comparison to TIA SCS 9001

CMMC is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the defense industrial base. CMMC is mandatory for all DoD contractors and subcontractors. CMMC leverages requirements from NIST SP 800-171 for its defined practices. CMMC does not provide specific support for supply chain risk management. The standard simply references NIST SP 800-161.

CMMC promotes a tiered maturity model, whereas TIA SCS 9001 is a process-based standard that provides extensive cybersecurity and supply chain security requirements and controls to provide assurance that a certifying organization practices proper security hygiene to provide assurance that their products and services are of inherently higher security.

TIA SCS 9001 focuses on securing the global supply chain for ICT products and services. TIA SCS 9001 provides nearly full coverage of all the practices defined within CMMC[2].

[2] This statement is accurate through CMMC Level 2. As of the writing of this version of this paper, CMMC Level 3 is under development and not yet available for evaluation.

CSA Cloud Controls Matrix

Snapshot

Publication Title:	Cloud Controls Matrix (CCM)
Publication Number:	V4.0.12
Publication Type:	Cybersecurity control framework for cloud computing
Primary Use Case:	Cybersecurity for cloud computing
Target Industry:	Cloud Computing
Current Version:	V4
Date of Last Release:	06/03/2024
Developing Organization(s):	Cloud Security Alliance (CSA)
Certifiable? (Yes / No):	Yes (Star Registry)
Where to get it:	Cloud Controls Matrix and CAIQ v4 | CSA (cloudsecurityalliance.org)
Free? (Yes / No):	Yes

Overview

CSA's CCM is a cybersecurity control framework that serves as a tool for the assessment of cloud implementations, offering guidance on the implementation of security controls within the cloud supply chain. The framework aligns with the CSA's Security Guidance for Cloud Computing and is recognized as a de-facto standard for cloud security assurance and compliance.

The CCM's structure allows for the mapping of its controls against widely accepted security standards, regulations, and control frameworks, such as ISO 27001/27002/27017/27018, NIST SP 800-53, and PCI DSS. This mapping facilitates a comprehensive approach to fulfilling various regulatory requirements through adherence to the CCM controls. Additionally, the CCM includes the Consensus Assessments Initiative Questionnaire (CAIQ), which provides a set of yes/no questions to assist in the assessment of cloud service providers, streamlining the evaluation process and reducing the need for multiple questionnaires.

A key feature of the CCM is its clarification of the shared responsibility model, delineating the responsibilities between cloud service providers (CSPs) and customers (CSCs). This demarcation aids organizations in understanding the relevance and implementation of each control within their cloud architecture. CSPs can also utilize the CCM to submit self-assessments to the STAR Registry, contributing to a transparent and trustworthy cloud ecosystem.

The CCM consists of 197 control objectives that are applied based on whether the deployed system is characterized as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS). These objectives are structured across the following domains that encompass all critical aspects of cloud technology.

1. Audit & Assurance (A&A)
2. Application & Interface Security (AIS)
3. Business Continuity Management & Operational Resilience (BCR)
4. Change Control & Configuration Management (CCC)
5. Cryptography, Encryption & Key Management (CEK)
6. Datacenter Security (DCS)
7. Data Security and Privacy Lifecycle Management (DSP)
8. Governance, Risk & Compliance (GRC)
9. Human Resources (HRS)
10. Identity & Access Management (IAM)
11. Interoperability & Portability (IPY)
12. Infrastructure & Virtualization Security (IVS)
13. Logging and Monitoring (LOG)
14. Security Incident Management, E-Discovery & Cloud Forensics (SEF)
15. Supply Chain Management, Transparency & Accountability (STA)
16. Threat and Vulnerability Management (TVM)
17. Universal Endpoint Management (UEM)

The CCM is accompanied by implementation guidelines that offer structured guidance on applying the controls, as well as auditing guidelines that provide resources for conducting CCM-related assessments. These documents support organizations in both implementing and verifying the effectiveness of these controls.

Comparison to TIA SCS 9001

The CCM provides a comprehensive set of security controls specifically designed for cloud computing environments. With its shared security responsibility model, the CCM is intended to be leveraged by both cloud service providers and their customers in managing the division of shared responsibility related to cloud security.

TIA SCS 9001 is a more general standard that is independent of the vertical industry, network architecture, or underlying technologies used to implement the network. TIA SCS 9001 has much more extensive capabilities that can be adopted to implement a comprehensive supply chain risk management strategy.

CCM and TIA SCS 9001 have considerable overlap, but each has strengths and specific capabilities in support of their defined purpose and use cases. Both may be used together to create more powerful outcomes for cloud computing environments than can be achieved by individual adoption.

ETSI EN 303 645

Snapshot

Publication Title:	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
Publication Number:	ETSI EN 303 645
Publication Type:	Standard
Primary Use Case:	High-level security and data protection provisions for consumer IoT devices.
Target Industry:	IoT
Current Version:	V3.1.2
Date of Last Release:	2024
Developing Organization(s):	European Telecommunications Standards Institute (ETSI)
Certifiable? (Yes / No):	Yes
Where to get it:	Search & Browse standards and download for free (etsi.org)
Free? (Yes / No):	Yes

Overview

ETSI's EN 303 645 aims to establish a security baseline for consumer IoT devices, addressing increasing concerns over consumer privacy and the exploitation of devices for malicious activities. The standard explicitly excludes devices that are not consumer IoT devices, such as those intended for use in manufacturing, healthcare, or other industrial applications.

EN 303 645 emphasizes the importance of incorporating baseline security into IoT products from the design phase and is based on 13 high-level recommendations, which translate into 68 provisions. Among these, there are 33 mandatory requirements and 35 recommendations that manufacturers should consider when designing and developing IoT products to enhance their resilience against cyber threats.

EN 303 645 is the result of collaboration among industry experts, academics, and government entities, and it has undergone a rigorous review and approval process by national standards organizations, further strengthening its provisions. The standard not only serves as a guideline for manufacturers but also provides a basis for future IoT certification schemes, ensuring a higher level of security for consumer IoT devices globally.

Comparison to TIA SCS 9001

EN 303 645 provides a baseline level for operational-level security and data protection of IoT devices. It is similar in capabilities to peer standards such as ANSI/CTA-2088-A and NIST IR 8425. ETSI states that the standard "specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope." Examples of the types of protections provided include:

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store sensitive security parameters
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is secure
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for users to delete their data
- Validate input data
- Data protection provisions

EN 303 645 has no equivalent for most of the cybersecurity and supply chain security capabilities required under TIA SCS 9001. In addition, TIA SCS 9001 is network, technology, and product independent—it does not include requirements for securing specific product categories such as consumer devices. TIA SCS 9001 is used to certify an organization and its security practices to provide assurance that the supplier can be trusted as a vendor.

TIA SCS 9001 and EN 303 645 are not competitive and can be used together to provide a more powerful outcome for IoT providers than either standard by itself.

GSMA Network Equipment Security Assurance Scheme (NESAS)

Snapshot

Publication Title:	Network Equipment Security Assurance Scheme (NESAS)
Publication Number:	Version 2.3
Publication Type:	Security Assurance Framework
Primary Use Case:	Mobile industry network equipment security
Target Industry:	Mobile networks
Current Version:	V2.3
Date of Last Release:	21 July 2023
Developing Organization(s):	Global System for Mobile Communications Association (GSMA)
Certifiable? (Yes / No):	Yes
Where to get it:	NESAS Documents - Industry Services (gsma.com)
Free? (Yes / No):	Yes

Overview

The NESAS is an industry framework designed to enhance security for mobile communications. Jointly developed by the 3GPP and GSMA, NESAS defines security requirements and provides an assessment framework for secure product development and product lifecycle processes. It also incorporates 3GPP-defined security test cases for the security evaluation of network equipment, ensuring that the equipment meets stringent security standards before deployment.

The scheme has evolved over time, with updates to reflect the changing security landscape and technological advancements. The latest version continues to build upon the robust framework established by previous versions, ensuring that the scheme remains relevant and effective.

NESAS is comprised of a set of the following specifications:

- GSMA PRD FS.13 Network Equipment Security Assurance Scheme – Overview
- GSMA PRD FS.14 Network Equipment Security Assurance Scheme Security Test Laboratory Accreditation
- GSMA PRD FS.15 Network Equipment Security Assurance Scheme Development and Lifecycle Assessment Methodology
- GSMA PRD FS.16 Network Equipment Security Assurance Scheme Development and Lifecycle Security Requirements
- GSMA PRD FS.46 Network Equipment Security Assurance Scheme Audit Guidelines

- GSMA PRD FS.47 Network Equipment Security Assurance Scheme Product and Evidence Evaluation Methodology
- 3GPP TR 33.916 Assurance Methodology for 3GPP network products
- 3GPP TS 33.117 Catalogue of General Security Assurance Requirements

NESAS defines a total of 20 requirements that focus on design security, source code management, software build system management, the development process, distribution of software, documentation, and customer communications.

Comparison to TIA SCS 9001

NESAS is intended to be used alongside other mechanisms to ensure a network is secure. It focuses on evaluating a vendor's development approach to delivering secure products. NESAS can be used as a common baseline, on top of which individual network operators or national IT security agencies may elect to define additional security requirements.

TIA SCS 9001 expands upon NESAS in defining requirements and controls to provide assurance of the operating practices of the entire organization, delivering products and services used to implement and administer modern networks. It has much more extensive requirements in managing the supply chain and cybersecurity in general.

TIA SCS 9001 and NESAS are not competitive; they are complementary and can be used together to deliver more powerful results than implementing either standard by itself.

ISO / IEC 20243

Snapshot

Publication Title:	Information Technology - Open Trusted Technology Provider Standard (O-TTPS) – Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products
Publication Number:	ISO/IEC 20243-1:2023(E)
Publication Type:	International Standard
Primary Use Case:	Supply chain security
Target Industry:	Information and Communications Technology
Current Version:	Second edition
Date of Last Release:	2023
Developing Organization(s):	Open Group
Certifiable? (Yes / No):	Yes
Where to get it:	ISO/IEC 20243-1:2023 - Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products
Free? (Yes / No):	No

Overview

ISO/IEC 20243, also known as O-TTPS, is a set of guidelines, requirements, and recommendations designed to mitigate the risks associated with maliciously tainted and counterfeit products within the ICT industry. The standard applies to the entire product life cycle, including design, sourcing, build, fulfillment, distribution, sustainment, and disposal. It aims to protect the integrity of commercial off-the-shelf (COTS) ICT products by addressing specific threats that can compromise hardware and software components.

ISO/IEC 20243 is particularly relevant for providers who are part of the supply chain for ICT products, offering practices that help in the identification and avoidance of tainted and counterfeit components. These practices include security labeling and other techniques to ensure the authenticity and safety of products. ISO/IEC 20243 is maintained by ISO/IEC, reflecting a global consensus on best practices for securing the technology supply chain. The

standard has undergone revisions to stay current with the evolving nature of threats and technology, with the latest version being ISO/IEC 20243-1:2023.

Comparison to TIA SCS 9001

ISO/IEC 20243 is a well-written standard and one of the limited examples of a modern, purpose-built standard targeting the ICT supply chain. ISO/IEC 20243 does this with a focus on development and supply chain assessments that consider the integrity of parts and components. The standard specifically states that its focus is to "enhance the security of the global supply chain and the integrity of COTS ICT products," and that it does so by providing "a set of guidelines, requirements and recommendations that help assure against maliciously tainted and counterfeit products."

TIA also promotes these goals, and accordingly, TIA SCS 9001 accounts for essentially all ISO/IEC 20243 requirements. TIA SCS 9001 builds upon ISO/IEC 20243 in providing an enhanced set of requirements and controls, delivered in a certifiable process-based standard, enabling an organization to evaluate the range of business processes of their suppliers.

TIA SCS 9001 is a Supply Chain Security Management System (SCSMS), which includes the goals of ISO/IEC 20243 in mitigating the risks of insecure products, but more importantly, fully assesses all security practices of an organization to provide evidence and documentation of the steps they have taken to become a reliable and trustworthy provider of secure products and services.

TIA SCS 9001 and ISO 20243 can both be leveraged as part of a comprehensive security management system. The two standards can be used in harmony through integrated certifications for time and cost efficiencies and more powerful outcomes than using either standard in isolation.

For a more detailed comparison, including specific mappings between the two publications, refer to the technical bulletin, TIA QuEST Forum's SCS 9001 Compared to ISO/IEC 20243.

IoXT Alliance

Snapshot

Publication Title:	ioXt <device type> Profile
Publication Number:	Various
Publication Type:	International Standard
Primary Use Case:	IoT Security
Target Industry:	IoT
Current Version:	2.0
Date of Last Release:	Various
Developing Organization(s):	ioXT
Certifiable? (Yes / No):	Yes
Where to get it:	https://www.ioxtalliance.org/certifying-your-device
Free? (Yes / No):	Yes (profile documents)

Overview

The ioXt Security Pledge outlines the following eight key principles for secure IoT product design and lifecycle management:

1. No Universal Passwords - devices must not use default or hardcoded passwords that are common across units.
2. Secured Interfaces - all device interfaces (e.g., Bluetooth, USB, network ports) must be protected against unauthorized access.
3. Automatic Security Updates - devices should support automatic updates to patch vulnerabilities quickly and efficiently.
4. Vulnerability Reporting Program - manufacturers must maintain a public process for reporting and addressing security vulnerabilities.
5. Security by Default - devices should ship with the most secure settings enabled by default.
6. Data Protection - personal and sensitive data must be encrypted and securely stored.
7. Product Lifecycle Management - manufacturers must disclose how long a device will receive security updates and support.
8. Transparency - clear documentation of security features and practices must be available to consumers and stakeholders.

The ioXT Security Pledge identifies the following profiles, each with a slightly different set of certification requirements:

- ioXt Base Profile
- ioXt Android Profile
- ioXt Smart Speaker Profile
- ioXt Mobile Application Profile
- ioXt Residential Camera Profile
- Network Lighting Controller Profile

Organizations can self-certify or pursue certification through an authorized lab.

Comparison to TIA SCS 9001

ioXt is focused on securing IoT devices across several defined profiles. The focus of these profiles is primarily operational security, but there are a limited number of organizational requirements, such as managing device end-of-life notifications and having a vulnerability management program.

TIA SCS 9001 is a more comprehensive standard that assesses an organization's operational practices, rather than individual devices, to provide assurance that its products and services are provided with a high level of security consideration.

The two standards could be used together to provide a stronger level of security assurance than individually.

ISO 27001 / 27002

Snapshot

Publication Title:	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Publication Number:	ISO/IEC 27001:2022
Publication Type:	Standard
Primary Use Case:	Requirements for establishing, implementing, maintaining and continually improving an information security management system.
Target Industry:	All
Current Version:	Third edition 2022-10
Date of Last Release:	October 25, 2022
Developing Organization(s):	International Standards Organization (ISO) and International Electrotechnical Commission (IEC)
Certifiable? (Yes / No):	Yes
Where to get it:	ISO/IEC 27001:2022 - Information security management systems — Requirements
Free? (Yes / No):	No

Overview

ISO/IEC 27001 is a prominent international standard used to implement Information Security Management Systems (ISMS), providing a systematic approach for organizations to manage confidential and sensitive corporate information. The standard “has been prepared to provide requirements for establishing, implementing, maintaining, and continually improving an information security management system.”

ISO/IEC 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 ISO and 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 to address evolving information security challenges. It provides a framework for establishing, implementing, maintaining, and continually improving an ISMS.

ISO 27001 is supported by the companion document, ISO 27002 Information security, cybersecurity and privacy protection — Information security controls. This document provides

guidance for selecting and implementing controls for information security risk treatment in an ISMS based on ISO 27001.

Comparison to TIA SCS 9001

ISO 27001 outlines the requirements for implementing an Information Security Management System (ISMS). It is a global standard with a specific focus on protecting Information and IT infrastructure, which is an important component of a comprehensive security management system.

In contrast, TIA SCS 9001 is a Supply Chain Security Management System (SCSMS) that addresses an even more challenging security problem and includes essentially all capabilities of ISO/IEC 27001.

TIA SCS 9001 and ISO/IEC 27001 can both be leveraged as part of a comprehensive security management system. TIA SCS 9001 can be viewed as a functional super-set of ISO/IEC 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.

For a more detailed comparison, including specific mappings between the two publications, refer to the technical bulletin, TIA QuEST Forum's SCS 9001 Compared to ISO/IEC 27001.

ISO 27017

Snapshot

Publication Title:	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
Publication Number:	ISO/IEC 27017:2015
Publication Type:	Standard
Primary Use Case:	Cybersecurity support for cloud services
Target Industry:	Cloud computing and services
Current Version:	Edition 1, 2015
Date of Last Release:	December, 2015
Developing Organization(s):	International Standards Organization (ISO) and International Electrotechnical Commission (IEC)
Certifiable? (Yes / No):	No
Where to get it:	ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
Free? (Yes / No):	No

Overview

ISO/IEC 27017 is a security standard within the ISO/IEC 27000 family, specifically designed to address the unique requirements of cloud services. It extends the guidelines of ISO/IEC 27002 by providing additional cloud-specific information security controls. This standard outlines a code of practice that helps both cloud service providers and users to establish a safer cloud-based environment, mitigating the risk of security issues.

It includes guidance on the roles and responsibilities between providers and customers, the handling of assets at the end of contracts, and the protection and separation of virtual environments, among other aspects. The implementation of ISO/IEC 27017's controls is based on a comprehensive risk assessment and considers legal, contractual, or regulatory requirements specific to the cloud sector.

ISO/IEC 27017 adds controls for the following cloud sector-specific concepts:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Comparison to TIA SCS 9001

ISO/IEC 27017 focuses on information security controls for cloud services, targeting both cloud service providers and their customers. It supplements ISO/IEC 27001 with the addition of cloud-specific guidance. It provides guidance but is not certifiable on its own.

TIA SCS 9001 is a more comprehensive standard that addresses cloud security considerations but goes much broader in providing assurance across the entire ICT supply chain.

The two standards can be leveraged together to deliver more powerful outcomes that meet the security needs of cloud service providers.

ISO 27032

Snapshot

Publication Title:	Cybersecurity — Guidelines for Internet Security
Publication Number:	ISO/IEC 27032:2023
Publication Type:	Standard
Primary Use Case:	Providing guidance to address Internet security issues based on social engineering, zero-day attacks, privacy, hacking and proliferation of malware, spyware and other malicious software.
Target Industry:	All organizations operating internet-connected systems
Current Version:	Edition 2, 2023
Date of Last Release:	June, 2023
Developing Organization(s):	International Standards Organization (ISO) and International Electrotechnical Commission (IEC)
Certifiable? (Yes / No):	No
Where to get it:	ISO/IEC 27032:2023 - Cybersecurity — Guidelines for Internet security
Free? (Yes / No):	No

Overview

ISO/IEC 27032:2012 is an international standard that provides guidelines for cybersecurity. It is designed to enhance the security of network and information systems, focusing on the critical aspects of cybersecurity and interdependence with other security domains such as information security, network security, internet security, and critical information infrastructure protection (CIIP).

The standard outlines a framework to foster collaboration among stakeholders by defining roles and offering guidance on addressing common cybersecurity issues. Its core principles establish baseline security practices and promote a collaborative approach to resolving cybersecurity challenges such as social engineering attacks, zero-day attacks, privacy attacks, hacking, and the proliferation of malicious software (malware), spyware, and other potentially unwanted software.

The guidance provided in ISO/IEC 27032:2012 encompasses both technical and non-technical controls for mitigating security risks. It covers:

- Preparing for attacks
- Preventing attacks
- Detecting and monitoring attacks
- Responding to attacks.

Given the scope of this document, the controls provided are at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within the document for further guidance. See Annex A for the correspondence between the controls cited in this document and those in ISO/IEC 27002.

Comparison to TIA SCS 9001

ISO/IEC 27032 is a helpful standard for providing operational security guidance in preparing for and managing common internet-based attacks. It does not compete with TIA SCS 9001.

TIA SCS 9001 is a much more comprehensive standard that can be used together with ISO/IEC 27032. It encompasses operational processes that align with the goals of ISO/IEC 27032, including incident risk management, vulnerability management, monitoring, patching, business continuity planning, and employee training.

ISO 28001

Snapshot

Publication Title:	Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance
Publication Number:	ISO 28001:2007(E) (reviewed and confirmed in 2021)
Publication Type:	Standard
Primary Use Case:	Physical supply chain, storage, and transportation protections
Target Industry:	All organizations operating internet-connected systems
Current Version:	Edition 1, 2007
Date of Last Release:	June, 2023
Developing Organization(s):	International Standards Organization (ISO)
Certifiable? (Yes / No):	No
Where to get it:	ISO 28001:2007
Free? (Yes / No):	No

Overview

ISO 28001 was introduced in 2007 by ISO/TC 8 (Ships and Marine Technology) and remains unchanged through its 2021 reaffirmation. It's designed to protect physical supply chains, with a strong emphasis on shipping, cargo integrity, and conveyance security. It is a concise standard, at just 34 pages, and centers on 31 requirements, nearly half of which focus on transportation logistics.

While ISO 28001 is well-suited for maritime, freight, and traditional supply chain nodes, it has not evolved to address modern cyber threats, digital supply chains, or ICT-specific vulnerabilities.

Comparison to TIA SCS 9001

ISO 28001 is a legacy standard that is narrowly focused on physical logistics and cargo protection. TIA SCS 9001 is a next-generation, comprehensive framework that not only subsumes ISO 28001's strengths but also extends far beyond, making it the clear choice for ICT organizations seeking audit-ready, cyber-resilient supply chain assurance

For a more detailed comparison, refer to the technical bulletin, Comparing SCS 9001 to ISO 28001.

ISO / SAE 21434

Snapshot

Publication Title:	Road vehicles — Cybersecurity engineering
Publication Number:	ISO/SAE 21434:2021
Publication Type:	Standard
Primary Use Case:	Cybersecurity for road vehicles
Target Industry:	Automotive
Current Version:	2021
Date of Last Release:	August 31, 2021
Developing Organization(s):	International Standards Organization (ISO) and SAE International (SAE)
Certifiable? (Yes / No):	Yes[3]
Where to get it:	ISO/SAE 21434:2021 - Road vehicles — Cybersecurity engineering
Free? (Yes / No):	No

Overview

ISO/SAE 21434 is a standard focused on cybersecurity engineering for road vehicles. In 2016, the ISO established a technical committee, ISO/TC 22/SC 32/WG 11, to develop standards related to cybersecurity for road vehicles. The standard was developed in collaboration with SAE International, leveraging their expertise in automotive engineering.

ISO/SAE 21434 was officially published in August 2021. It provides a comprehensive framework for managing cybersecurity risks throughout the lifecycle of road vehicles. The standard aims to ensure that cybersecurity is considered at every stage of a vehicle's lifecycle, from design and development to production, operation, and decommissioning. It includes guidelines for risk assessment, threat management, and the implementation of security controls.

This standard is essential for addressing the growing cybersecurity challenges in the automotive industry and is especially important considering the increasing levels of connectivity and complexity of modern vehicles.

[3] ISO/SAE 21434 is certifiable, though it's not a traditional management system standard. Instead, certification typically involves a conformity assessment or audit conducted by recognized third parties.

Comparison to TIA SCS 9001

ISO/SAE 21434 and TIA SCS 9001 are both standards that address cybersecurity concerns, but they serve different aspects within the field. ISO/SAE 21434 focuses on cybersecurity engineering for road vehicles, providing a framework for managing cybersecurity risks throughout the lifecycle of electrical and electronic systems in vehicles. It emphasizes the importance of considering cybersecurity at every stage of product development, from concept to decommissioning.

In comparison, TIA SCS 9001 is a supply chain security management system standard, which is specifically designed to tackle threats within the supply chain of information and communications technology (ICT).

While ISO/SAE 21434 is focused on the automotive industry, TIA SCS 9001 has a broader application across various industries that rely on ICT. Increasingly, connected vehicles employ common technology components, including open-source software. The industry must improve security, especially with the emergence of connected, autonomous vehicles.

TIA SCS 9001 can play an essential role in ensuring that suppliers to automobile manufacturers practice the requisite level of organizational security to ensure the products, technologies, and services being deployed in modern vehicles meet stringent security expectations.

MITRE System of Trust (SoT)

Snapshot

Publication Title:	System of Trus™ (SoT)
Publication Number:	N/A
Publication Type:	Framework
Primary Use Case:	Supply Chain Security
Target Industry:	All
Current Version:	1.3
Date of Last Release:	June 24, 2023
Developing Organization(s):	MITRE Corporation
Certifiable? (Yes / No):	No
Where to get it:	System of Trust™ (mitre.org)
Free? (Yes / No):	Yes

Overview

The MITRE Corporation's System of Trust™ (SoT) is a comprehensive framework designed to enhance supply chain security through a risk assessment process. It provides organizations with a method to evaluate the trustworthiness of their suppliers, supplies, and service providers. The SoT framework encompasses 14 risk areas, guiding organizations in assessing over 2,200 specific supply chain security risk questions. These questions help determine how well each supplier manages the integrity and security of their software, hardware, services, and organizational structures.

The SoT Framework builds a basis of trust within three main aspects of supply chain security—suppliers, supplies, and services. It identifies and addresses the 14 top-level decisional risk areas with each of these three aspects to help agencies and enterprises make informed choices during the full life cycle of their acquisition activities.

The framework draws upon numerous data repositories to advance a probabilistic risk assessment of the trustworthiness of a product, service, or supplier. SoT guides the user through a series of questions that refine the risks and sub-risks for their specific use cases. SoT also offers predefined profiles for everyday use cases.

Comparison to TIA SCS 9001

The MITRE SoT is a general-purpose framework designed for use in any industry. It was developed to address supply chain security challenges by providing a comprehensive, consistent, and repeatable methodology for evaluating the trustworthiness of suppliers, supplies, and service providers.

The MITRE SoT is not a certifiable standard in the traditional sense. It is a risk assessment framework designed to help organizations evaluate supply chain trustworthiness using a structured, evidence-based approach.

TIA SCS 9001 is a certifiable, process-based standard developed for the needs of the ICT industry. The MITRE SoT Risk Domains map to requirements within TIA SCS 9001 for ICT use cases. The publications can be used together to more fully assess and mitigate risks in supply chains.

NIST SP 800-161r1

Snapshot

Publication Title:	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
Publication Number:	SP 800-161r1
Publication Type:	Special Publication
Primary Use Case:	Cybersecurity Supply Chain Risk Management
Target Industry:	Various, but originally developed for federal agencies to manage supply chain risks associated with information and communication technology (ICT) products and services.
Current Version:	Revision 1
Date of Last Release:	May, 2022
Developing Organization(s):	National Institute of Standards and Technology (NIST)
Certifiable? (Yes / No):	No
Where to get it:	NIST.SP.800-161r1.pdf
Free? (Yes / No):	Yes

Overview

NIST 800-161r1 is a comprehensive guide that addresses cybersecurity risks in supply chain management for systems and organizations. It provides a framework for identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of an organization. The document emphasizes the importance of integrating cybersecurity supply chain risk management (C-SCRM) into overall risk management activities. It outlines a multilevel approach to C-SCRM, which includes developing strategy implementation plans, policies, and risk assessments for products and services.

The latest revision of the NIST Special Publication builds upon previous guidelines and incorporates new insights and practices that have emerged in the field. It is a critical resource for enterprise risk management and C-SCRM owners and operators, as well as for those involved in acquisition, procurement, information security, system development, and implementation. The publication also addresses growing concerns about the risks associated with products and services that may contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. By following the guidance provided in NIST 800-161r1, organizations can enhance the security, resilience, reliability, safety, integrity, and quality of their products and services.

Comparison to TIA SCS 9001

NIST SP 800-161r1 is a comprehensive, non-certifiable guide for embedding C-SCRM across federal and commercial ecosystems. It's ideal for strategy formation, acquisition vetting, and policy alignment.

NIST SP 800-161r1 and TIA SCS 9001 are complementary, not mutually exclusive. Organizations can use NIST SP 800-161r1 to set strategy while relying on TIA SCS 9001 as the auditable execution layer. They serve different but overlapping purposes in the cybersecurity supply chain ecosystem:

- NIST SP 800-161r1 helps you design and implement a C-SCRM strategy.
- TIA SCS 9001 operationalizes and certifies the developed strategy within ICT supply chains.

NIST SP 800-53

Snapshot

Publication Title:	Security and Privacy Controls for Information Systems and Organizations
Publication Number:	SP 800-53
Publication Type:	Special Publication
Primary Use Case:	Manage and secure information systems
Target Industry:	Originally designed for U.S. federal agencies but adapted since the 5th edition to be applied by organizations across various industries.
Current Version:	5.1.1
Date of Last Release:	November 27, 2023
Developing Organization(s):	National Institute of Standards and Technology (NIST)
Certifiable? (Yes / No):	No
Where to get it:	NIST.SP.800-53r5.pdf
Free? (Yes / No):	Yes

Overview

NIST 800-53 is a comprehensive set of security and privacy controls for federal information systems and organizations, designed to ensure the confidentiality, integrity, and availability of system-related information. The publication provides guidelines for selecting and specifying security controls for organizations to protect their information and information systems from a diverse set of threats, including hostile cyberattacks, natural disasters, structural failures, and human errors. The latest revision includes updates and clarifications to the controls, introduces new control identifiers with leading zeros for consistency, and adds new controls related to identity providers and token management. It also provides mappings and crosswalks to other frameworks and standards, which can be particularly useful for organizations looking to align with multiple compliance requirements.

NIST 800-53 is part of the Special Publication 800-series, which reports on research, guidelines, and outreach efforts in information system security through NIST's Information Technology Lab (ITL) and assists federal agencies in implementing the Federal Information Security Modernization Act of 2014 (FISMA). NIST 800-53 is essential for federal agencies and any enterprises providing cloud-hosted services to a federal agency that stores classified data,

offering a catalog of controls that support the development of secure and resilient federal information systems.

NIST Special Publication 800-53 was initially designed for U.S. federal agencies to help them manage and secure their information systems. However, since its fifth revision, it has been adapted for general usage and can be applied by organizations across various industries to enhance their cybersecurity practices.

Comparison to TIA SCS 9001

NIST SP 800-53 and TIA SCS 9001 both target cybersecurity and supply chain resilience, but they approach those goals from different angles. NIST SP 800-53 serves as an extensive control catalog, providing a master list of security and privacy safeguards meant for federal systems but widely adopted across industries. It's designed to be flexible, enabling organizations to select and tailor controls based on their risk environment, operational mission, and compliance needs. There are over a thousand controls grouped into 20 families, such as Access Control, System Integrity, and Risk Assessment, each accompanied by assessment procedures (in 800-53A) that support internal or third-party reviews.

TIA SCS 9001 is a certifiable, ICT-focused standard to address cyber and supply chain security challenges. Using both documents together provides depth and structure. NIST SP 800-53 can serve as the strategic design backbone for ensuring a comprehensive control environment that guides internal security architecture, procurement policies, and assessment frameworks. TIA SCS 9001 then becomes the execution layer, ensuring processes that operationalize the controls for network operators and vendors in the ICT vertical.

Organizations that elect to leverage both documents can use SP 800-53 to define the baseline security requirements for suppliers, including expectations around software provenance, incident handling, and access control. They can then mandate that suppliers demonstrate conformance through TIA SCS 9001 certification, ensuring that those controls are not just theoretical but embedded in daily operations.

NIST Cybersecurity Framework (CSF) 2.0

Snapshot

Publication Title:	The NIST Cybersecurity Framework (CSF) 2.0
Publication Number:	N/A
Publication Type:	Framework
Primary Use Case:	Guidance to industry, government agencies, and other organizations to manage cybersecurity risks.
Target Industry:	Any
Current Version:	2.0
Date of Last Release:	February 26, 2024
Developing Organization(s):	National Institute of Standards and Technology (NIST)
Certifiable? (Yes / No):	No
Where to get it:	NIST.CSWP.29.pdf
Free? (Yes / No):	Yes

Overview

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It provides a taxonomy of high-level cybersecurity outcomes that organizations of all sizes and sectors can use to better understand, assess, prioritize, and communicate their cybersecurity efforts. The framework does not prescribe how to achieve outcomes; instead, it provides links to online resources that offer guidance on best practices and controls.

The CSF was established in response to cybersecurity risks, particularly those that pose a threat to critical infrastructure. Its development was mandated by Executive Order 13636, issued on February 12, 2013, which tasked NIST with developing a standardized security framework. NIST took a collaborative approach, gathering input from government, industry, and academia through Requests for Information (RFIs) and Requests for Comment (RFCs). This inclusive process ensured the framework would be comprehensive and widely applicable.

The initial release of CSF in 2014 was built around five core functions: Identify, Protect, Detect, Respond, and Recover. This structure provides a high-level taxonomy of outcomes and a strategic view of the entire lifecycle of managing cybersecurity risk. The CSF is designed to be flexible, allowing organizations to adapt it to their specific needs and risk profiles.

The CSF serves as a voluntary guide to help organizations manage and reduce cybersecurity risks while protecting their networks and data. It outlines a set of best practices and desired outcomes for organizations to prioritize their efforts effectively. For instance, the CSF can be customized to create community profiles, which are tailored implementations of the framework that address the unique needs and risk landscapes of specific communities or sectors.

Updates in NIST CSF Version 2.0

Released in February 2024, CSF 2.0 is the first major revision of the framework since its debut in 2014. It was developed over several years with input from public comments and discussions surrounding the latest cybersecurity challenges and management practices. TIA actively participated in the review and provided comments on proposed changes.

The transition from CSF 1.0 to 2.0 marks an evolution in the approach to cybersecurity. The latest release expands its applicability beyond critical U.S. infrastructure to apply to organizations of all sizes and industries globally. This broader focus recognizes that cybersecurity threats are universal, and a standardized approach is required to manage them. A key addition in CSF 2.0 is the Govern function, which complements the existing five functions: Identify, Protect, Detect, Respond, and Recover. This new function highlights the importance of governance and strategic cybersecurity decision-making at the senior leadership level. CSF 2.0 also introduces a new category, the Identify function, which focuses on continuous improvement. This emphasizes the need for organizations to regularly update their cybersecurity profiles and action plans in response to the ever-evolving threat landscape. Lastly, CSF 2.0 strengthens its guidance with new subcategories that address risk appetite, tolerance, supply chain, and response options.

Comparison to TIA SCS 9001

NIST CSF 2.0 is a voluntary, strategic framework that helps organizations manage cybersecurity risk through its six core functions. It's ideal for organizations seeking a flexible, risk-based approach to cybersecurity, especially in multi-sector environments. It's widely adopted for its simplicity and adaptability, especially in regulatory contexts like Executive Order 14028 and the Securities and Exchange Commission (SEC) cyber disclosure rule.

In contrast, TIA SCS 9001 is a process-based standard specifically for ICT organizations. It provides a certifiable framework for operationalizing cybersecurity and supply chain security. TIA SCS 9001 does not replace NIST CSF but instead builds upon it. While CSF provides a risk-based approach, SCS 9001 offers certifiable, process-based requirements and controls that can help organizations operationalize and certify their existing CSF practices.

For a more detailed comparison, including specific mappings between the two publications, refer to the technical bulletin, NIST Cyber Security Framework R2 and SCS 9001.

NIST NISTIR 8276

Snapshot

Publication Title:	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
Publication Number:	NIST Internal Report (NISTIR) 8276
Publication Type:	Internal Report
Primary Use Case:	Managing cybersecurity risk in supply chains.
Target Industry:	Any
Current Version:	N/A
Date of Last Release:	February, 2021
Developing Organization(s):	National Institute of Standards and Technology (NIST)
Certifiable? (Yes / No):	No
Where to get it:	NIST.IR.8276.pdf
Free? (Yes / No):	Yes

Overview

NISTIR 8276 is a comprehensive report that outlines a set of key practices organizations of any size, scope, and complexity can adopt to manage cybersecurity risks associated with their supply chains. The report emphasizes the importance of integrating a formal Cyber Supply Chain Risk Management (C-SCRM) program throughout an organization, highlighting the need for organizations to know and manage their critical components and suppliers, understand their supply chain, and closely collaborate with key suppliers. Additionally, it suggests including suppliers in resilience and improvement activities, assessing and monitoring suppliers throughout the entire relationship, and planning for the whole life cycle of products and services. These practices are based on extensive research and resources from both government and industry, including research conducted by NIST in 2015 and 2019. The document serves as a valuable resource for digital businesses looking to fortify their defenses against cyber threats in today's interconnected world.

NISTIR 8276 outlines desirable outcomes for organizations to strive for, but does not dictate methods for achieving them. Guidance on practices and controls that can be used to reach desired outcomes is provided in a suite of online resources available through the NIST CSF website. These resources are intended to help an organization understand, adopt, and use the CSF.

Comparison to TIA SCS 9001

NISTIR 8276 is a guidance document, not a standard. It distills industry observations into best practices. TIA SCS 9001 is built to fulfill NISTIR 8276's intent. It doesn't compete—it implements. NISTIR 8276 outlines what organizations should consider (e.g., supplier integrity, lifecycle risk, incident response) while TIA SCS 9001 defines how to do it with the capability of independent auditing and certification.

For a more detailed comparison, refer to the technical bulletin, How TIA QuEST Forum's SCS 9001 Operationalizes the NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management: Observations from Industry.

NIST IR 8425

Snapshot

Publication Title:	**Profile of the IoT Core Baseline for Consumer IoT Products**
Publication Number:	NISTIR 8425
Publication Type:	Internal Report
Primary Use Case:	IoT Operational Security
Target Industry:	Consumer Devices
Current Version:	Initial release
Date of Last Release:	September, 2022
Developing Organization(s):	National Institute of Standards and Technology (NIST)
Certifiable? (Yes / No):	No
Where to get it:	NIST.IR.8425.pdf
Free? (Yes / No):	Yes

Overview

Published in September 2022, NISTIR 8425 outlines cybersecurity capabilities essential for consumer IoT products. The report was developed in response to Executive Order 14028 and is part of a broader effort to provide guidelines for the cybersecurity labeling of consumer IoT products. It serves as a consumer profile of NIST's IoT core baseline, focusing on IoT devices intended for home or personal use and providing a framework for understanding the cybersecurity features that should be present in consumer IoT products to ensure their safety and privacy. The consumer profile is expressed through cybersecurity outcomes that apply to the entire IoT product lifecycle.

NIST IR 8425 is a valuable resource for small businesses and other stakeholders when considering the purchase and implementation of IoT products. It emphasizes the importance of secure and privacy-respecting IoT devices in today's interconnected world. The document also includes insights from a comprehensive review of relevant source documents and stakeholder engagement over a year-long period. By establishing a clear set of capabilities, NISTIR 8425 aims to guide manufacturers and consumers towards a common understanding of what constitutes a secure IoT product.

Finally, NISTIR 8425 provides the technical criteria that underpin the cybersecurity labeling framework for consumer IoT devices within the U.S. Cyber Trust Mark program.

Comparison to TIA SCS 9001

NISTIR 8425 and TIA SCS 9001 represent two distinct but complementary approaches to cybersecurity in the digital ecosystem. NISTIR 8425 is a guidance document that outlines cybersecurity outcomes for consumer IoT products and serves as the technical foundation for the U.S. Cyber Trust Mark labeling program. Its goal is to help manufacturers of smart home devices—thermostats, cameras, and routers—embed baseline security features such as secure software updates, data protection, and access control. The outcomes are broad and flexible, designed to be adapted across various consumer IoT technologies and use cases.

In contrast, TIA SCS 9001 goes far beyond consumer devices, addressing cybersecurity and supply chain integrity across the entire lifecycle of networking and communications hardware, software, and services. TIA SCS 9001 is process-based and supports formal audits through its certification program.

Where NISTIR 8425 is outcome-driven and voluntary, TIA SCS 9001 is requirement-driven and certifiable. NIST's framework is ideal for manufacturers seeking to meet minimum cybersecurity expectations and participate in labeling programs. TIA SCS 9001, on the other hand, is designed for network operators, manufacturers, and service providers in the ICT industry who need to demonstrate rigorous cybersecurity and supply chain controls to regulators, partners, and customers.

UL 2900

Snapshot

Publication Title:	ANSI/UL 2900-1 Software Cybersecurity
Publication Number:	N/A
Publication Type:	Standard
Primary Use Case:	Electronic devices
Target Industry:	Medical originally, now adapted to numerous others (see below)
Current Version:	UL 2900-1:2023
Date of Last Release:	April 14, 2023
Developing Organization:	UL Solutions
Certifiable? (Yes / No):	Yes
Where to get it:	UL 2900-1 | UL Standards & Engagement | UL Standard (shopulstandards.com)
Free? (Yes / No):	No

Overview

UL 2900 is a series of standards developed by UL Solutions to provide a framework for evaluating and testing the cybersecurity of network-connected devices. These standards are designed to help manufacturers identify and mitigate potential security vulnerabilities and exploits in their products. The UL 2900 standards series include several parts, each targeting different product categories or aspects of cybersecurity. For instance, UL 2900-1 outlines general requirements for software cybersecurity, while UL 2900-2-1 focuses on healthcare systems, and UL 2900-2-2 addresses industrial control systems.

The standards are recognized by the American National Standards Institute (ANSI) and have been adopted by the U.S. Food and Drug Administration (FDA) for the premarket and post-market management of cybersecurity in medical devices. They align with the FDA's guidance on the content of premarket submissions for the management of cybersecurity in medical devices and post-market management. UL 2900 encourages a risk management approach, considering the core functions of the NIST Cybersecurity Framework.

Comparison to TIA SCS 9001

UL 2900 is a product-focused cybersecurity standard. It provides technical requirements for evaluating the security of software-based systems, including industrial controls, medical devices, and life safety systems. The standard is modular, with UL 2900-1 offering general cybersecurity criteria, and extensions like UL 2900-2-1 and UL 2900-2-2 targeting specific sectors. Recognized by ANSI and the FDA, UL 2900 is particularly relevant in regulated environments where device-level security must be validated before deployment.

In contrast, TIA SCS 9001 is a process-based, certifiable management system standard. It's designed for organizations across the ICT supply chain—network operators, manufacturers, integrators, and service providers—who need to demonstrate cybersecurity and supply chain integrity at scale. TIA SCS 9001 doesn't evaluate individual products; it assesses how an organization manages cyber risk across its operations, suppliers, and lifecycle processes. It is suitable for enterprise-level certification and continuous improvement.

The key difference lies in scope and granularity. UL 2900 zooms in on the security posture of individual products, testing for vulnerabilities, secure coding practices, and resilience against known threats. TIA SCS 9001 zooms out to assess the organizational systems that govern how products are developed, sourced, deployed, and maintained.

UL 2900 and TIA SCS 9001 do not directly compete; they serve different layers of cybersecurity assurance. In some cases, they can be complementary. UL 2900 is about certifying the security of what you build, while TIA SCS 9001 is about certifying how you build and manage it.

Get involved with SCS 9001

Interested in joining our Supply Chain Security Working Group? Join leaders from global network providers, equipment suppliers, cloud solutions providers, software developers, connected device manufacturers and consultants to evolve SCS 9001 to meet the ever-changing cybersecurity and supply chain risk management (SCRM) landscape.

To get involved, contact us at supplychainsecurity@tiaonline.org

Learn more at: https://tiaonline.org