ETSI TR 103 937 V1.1.1 (2024-08)

TECHNICAL REPORT

Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management

Reference

DTR/CYBER-0099

Keywords

cyber security, cyber-defence, risk management

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The development of tools for cyber resiliency under a broad "Zero Trust Model" aegis continue evolve and include Supply Chain Bill of Materials (SBOM), community exchange of vulnerability and remediation code, Continuous Monitoring for threat anomalies, and application of Critical Security Controls.

Introduction

Over the past several years, the increasing significant attacks on ICT infrastructure has led to a return to cybersecurity fundamentals developed after the conceptualization of packet data networks to provide access to computer resources. It was a realization that persistent vulnerabilities in every digital element and system will always exist, that "ex ante" trust certifications were minimally useful, and that a different set of tools was necessary. The development of these tools for cyber resiliency proceeded under a broad "Zero Trust Model" aegis that includes Supply chain Bill Of Materials (SBOM), community exchange of vulnerability and remediation code, Continuous Monitoring for threat anomalies, and application of Critical Security Controls.

1 Scope

The present document addresses cyber resiliency throughout the supply chain and the various related frameworks and measures using risk-based, system of trust, and zero trust approaches, including the proposed EU Cyber Resilience Act, [i.1] through [i.8].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

[i.2] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

[i.3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

[i.5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[i.6] Consolidated text: Commission Delegated Regulation (EU) 2021/2106 of 28 September 2021 on supplementing Regulation (EU) 2021/241 of the European Parliament and of the Council establishing the Recovery and Resilience Facility by setting out the common indicators and the detailed elements of the recovery and resilience scoreboard.

[i.7] United Kingdom: "Product Security and Telecommunications Infrastructure Act 2022".

[i.8] Switzerland: "120.73 Ordinance of 27 May 2020 on Protection against Cyber Risks in the Federal Administration (Cyber Risks Ordinance, CyRV)".

[i.9] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[i.10] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.11] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.12] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.13] NIST SP 800-161r1: "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations".

[i.14] MITRE: "System of Trust™: Supply Chain Security".

[i.15] NIST SP 800-207: "Zero Trust Architecture".

[i.16] 3GPP TR 33.894: "Technical Specification Group Services and System Aspects; Study on applicability of the Zero Trust Security principles in mobile networks (Release 18)".

[i.17] Cloud Security Alliance, Zero Trust publications.

[i.18] NIST NCCoE: "Implementing a Zero Trust Architecture".

[i.19] CISA: "Zero Trust Maturity Model", Version 2.0.

[i.20] National Security Agency: "Cybersecurity Information: Embracing a Zero Trust Security Model".

[i.21] NCSC: "Zero trust architecture design principles".

[i.22] ITU-T: "MITRE"s System of Trust™, Software Supply Chair Risks That May Need to Be Addressed".

[i.23] IETF RFC charter-ietf-scitt: "Supply Chain Integrity, Transparency, and Trust (scitt)".

[i.24] IETF RFC draft-ietf-scitt-architecture: "An Architecture for Trustworthy and Transparent Digital Supply Chains".

[i.25] US ODNI, NSA, CISA: "Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption".

[i.26] NCSC: "Guidelines for secure AI system development".

[i.27] NSA: "Advancing Zero Trust Maturity Throughout the Device Pillar".

[i.28] GSMA: "Supply Chain Toolbox".

[i.29] NTIA: "Software Bill of Materials".

[i.30] ITU-T TR.zt-acp: "Technical Report on Guidelines for zero trust based access control platform in telecommunication networks".

[i.31] ITU-T X.st-ssc: "Security threats of software supply chain".

[i.32] CISA: "Information and Communications Technology Supply Chain Security".

[i.34] U.S. Executive Office of the President, NSM-22: "National Security Memorandum on Critical Infrastructure Security and Resilience", 30 April 2024.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

cyber resiliency: ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources

NOTE: As defined in NIST SP 800-161r1 [i.13].

cybersecurity risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

NOTE: As defined in [i.1] and [i.3].

software bill of materials: formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships

supply chain: linked set of resources and processes between and among multiple levels of an enterprise, each of which is an acquirer that begins with the sourcing of products and services and extends through the product and service life cycle

NOTE: As defined in NIST SP 800-161r1 [i.13].

supply chain risk management: potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services - which are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself

NOTE: As defined in NIST SP 800-161r1 [i.13].

system of trust: framework aimed at defining, aligning, and addressing the specific concerns and risks that stand in the way of organizations' trusting suppliers, supplies, and service providers

vulnerability exploitability eXchange: concept and format created through a multistakeholder process for software component transparency used to implement Software Bills Of Materials (SBOM)

zero trust: collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised

NOTE: As defined in NIST SP 800-207 [i.15].

zero trust architecture: architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized

NOTE: As defined in [i.18].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BMI	Bundesministerium des Innern und für Heimat (Germany)
BoK	Body of Knowledge
BSI	Bundesamt für Sicherheit in der Informationstechnik

CISA	Cybersecurity and Infrastructure Security Agency
CSA	Cloud Security Alliance
C-SCRM	Cybersecurity Supply Chain Risk Management
EU	European Union
GSMA	GSM Association
IAM	Identity and Access Management
MPCVD	Multi-Party Coordinated Vulnerability Disclosure
NCCoE	National Cyber security Center of Excellence
NCSC	National Cyber Security Centre
NIST	National Institute for Standards and Technology
NSA	National Security Agency (US)
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration (US)
ODNI	Office of the Director of National Intelligence (US)
SBOM	Software Bill Of Materials
SCITT	Supply Chain Integrity, Transparency and Trust
SEI	Software Engineering Institute (US Carnegie-Mellon University)
SME	Small or Medium Enterprise
SoT	System of Trust
SP	Special Publication
VEX	Vulnerability Exploitability eXchange
ZTA	Zero Trust Architecture
ZTaaS	Zero Trust as a Service
ZTMM	Zero Trust Maturity Model

4 Concepts and model frameworks

4.1 Cyber resiliency

The concept of cyber resiliency has a long history typically associated with national critical infrastructure and emergency preparedness. The requirements for resiliency are threaded through global and national telecommunication activities and instruments throughout the long arc of communication history and public networks in nearly every nation included considerable attention and resources to maximizing resiliency. Resilience is the ability of a system to recover and resume operations, or to continue to operate, in the face of adversity - arising from chance conditions or intentional actions. Cyber resilience incorporates the traditional approaches to cybersecurity with a broader emphasis on the prevention of and recovery from malicious attacks.

A focus on cyber resiliency emerged over the past several decades as communication infrastructure became provided largely by private enterprise in relatively unencumbered marketplaces and much more complex - both factors resulting in substantial diminishing resiliency of systems and products. As corrective measures, national authorities have adopted corrective measures in the form of regulatory and executive mandates, refer to [i.1] to [i.9] and [i.34].

Because cyber resiliency is an elusive, constantly evolving, and ultimately unattainable objective, the manifestation of those mandates have given rise to improving the trust of products and systems through supply chain risk management practices described below that are tailored to the criticality of infrastructures and levels of assumed risk.

4.2 Supply chain risk management

4.2.1 Government-driven supply chain risk management model frameworks

EU - NIS2. The EU NIS2 Directive (Directive (EU) 2022/2555) [i.3] includes in its explanatory preamble as well as the body of the text, numerous statements and requirements directed at supply chain risk management.

EU - Cyber Resilience Act. The relevant Union legislation that is currently in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, the existing Union legislation related to cybersecurity, including NIS2 [i.3] and the Cybersecurity Certification Act [i.9] do not directly cover mandatory requirements for the security of products with digital elements. The Cyber Resilience Act [i.1], which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under NIS2 by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

USA - CISA [i.32]. CISA has emerged as the global leader for ICT resilience and supply chain security through the exchange of information and development and orchestration of the frameworks and tools necessary to meet the challenges. A key component is the SBOM platform originally developed through an NTIA industry collaborative process described below.

USA - NTIA [i.29]. A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access-restricted. In today's world, software touches every part of our life and spans across industries, with much of it built on third-party code and open source software. Any organization concerned about better supporting their software products internally, supporting their customers, and positively differentiating themselves in the marketplace should consider creating SBOM and providing them to support their customers.

USA - NIST [i.13]. Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services. Guidance to organizations is necessary on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. A focus is necessary on integrating Cybersecurity Supply Chain Risk Management (C-SCRM) into risk management activities by applying a multilevel, C-SCRM-specific approach, including guidance on the development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans and risk assessments for products and services.

USA - ODNI, NSA, CISA. The multiple initiatives and increasing need for definitive software supply chain security practices in the USA led ultimately to publication of Recommended Practices for Software Bill of Materials [i.25]. The three-agency publication is comprised by a discussion of SBOM and risk scoring, how to operationalize and scale the use of SBOM, SBOM lifecycles in the enterprise, and almost every element of enhancing resiliency through the use of these techniques.

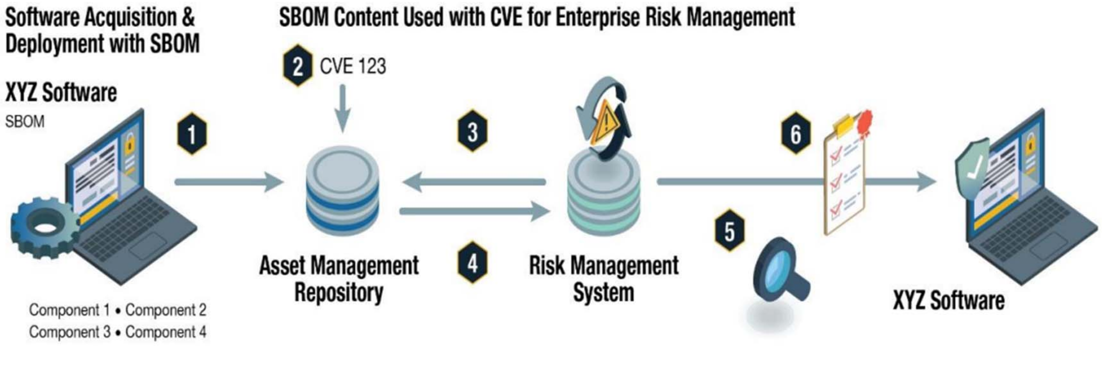

Software Acquisition & Deployment with SBOM
SBOM Content Used with CVE for Enterprise Risk Management
XYZ Software
SBOM
2 CVE 123
1
3
6
5
4
Asset Management Repository
Risk Management System
XYZ Software
Component 1 • Component 2
Component 3 • Component 4

**Figure 4.2.1-1: Example of SBOM in Use
(Source: [i.25])**

NCSC - Guidelines for secure AI system development. The rapid emergence and scaling use of Artificial Intelligence (AI) software and systems led 22 national security agencies together with 19 private sector commercial and nonprofit institutions to develop a set of guidelines to develop AI supply chain risk management practices [i.26]. The practices encompass:

1) secure design;

2) secure development including the supply chain;

3) secure deployment; and

4) secure operation and maintenance.

4.2.2 Industry-developed supply chain risk management model frameworks

GSMA [i.28]. Mobile operators rely on different suppliers to deliver the necessary infrastructure, components and solutions to create products and services resulting in supply chains being large and complex. Operators need to be able to ensure that its supply chain does not compromise security. However, securing the supply chain can be hard because vulnerabilities can be inherited or introduced and exploited at any point in the supply chain. Attackers do not need to attack an operator's network directly they can, in many cases, achieve their aims by attacking the weakest point in the supply chain. The GSMA Supply Chain Toolbox outlines a number of services and guidelines to help operators and their suppliers to better understand security and to access best practice. This includes different accreditation and assurance schemes and guidelines pertaining to specific areas of mobile technology. The different resources in the toolbox are organized by relevance to the different stages of procurement by an operator and to different stages of a vendor's solution lifecycle.

MITRE [i.14]. The System of Trust (SoT) Framework is the foundation needed for understanding supply chain risks and that it will be the key to securing robust and resilient supply chains, trustworthy partners, and trusted components and systems that are globally manufactured. The SoT Framework is aimed at defining, aligning, and addressing the specific concerns and risks that stand in the way of organizations' trusting suppliers, supplies, and service providers. More importantly, the framework offers a comprehensive, consistent, and repeatable methodology - for evaluating suppliers, supplies, and service providers alike - that is based on decades of supply chain security experience, deep insights into the complex challenges facing the procurement community of interest, and the community's broad knowledge of the supply chain as shown in literature and relevant standards organizations.

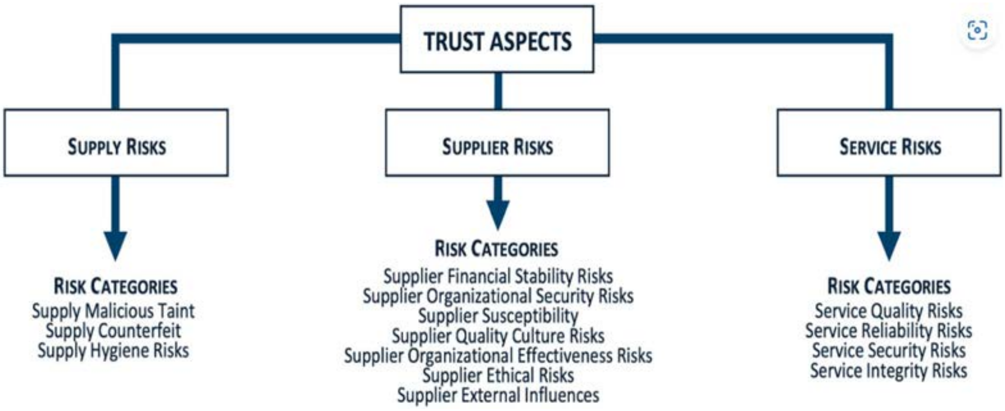
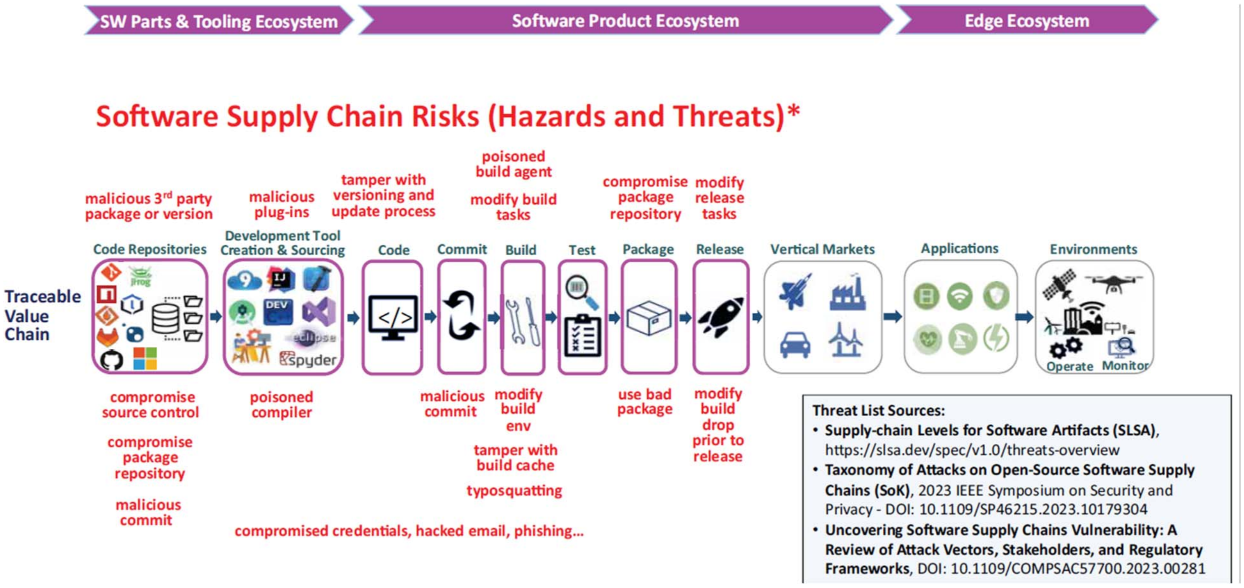


Figure 4.2.2-1: System of Trust, showing key risk areas (Source MITRE [i.14])

The four overarching components of the SoT Framework are:

- Body of Knowledge (BoK) -predefined profiles and questions used in SoT assessments.
- Assessment -predefined profile and questions to narrow down the SoT content to something appropriate to the product, service, or supplier in question and then aligned to the assessing organization's assessment focus, resources, available time, and legal authorities, and to its present acquisition challenge.
- Scoring - Risks are scored using a set of contextually driven, tailorable, weighted measurements that are used as inputs into a scoring algorithm that are used to identify supplier strengths and weaknesses against the applicable risk categories.
- Customization - ability to customize for specific use cases and user environments.

The software supply chain risks are depicted in Figure 4.2.2-2, below.



Threat List Sources:

- **Supply-chain Levels for Software Artifacts (SLSA)**, https://slsa.dev/spec/v1.0/threats-overview
- **Taxonomy of Attacks on Open-Source Software Supply Chains (SoK)**, 2023 IEEE Symposium on Security and Privacy - DOI: 10.1109/SP46215.2023.10179304
- **Uncovering Software Supply Chains Vulnerability: A Review of Attack Vectors, Stakeholders, and Regulatory Frameworks**, DOI: 10.1109/COMPSAC57700.2023.00281

Figure 4.2.2-2: Software Supply Chain Integrity, Transparency & Trust (Source ITU [i.22])

The entire ensemble of Supplier, Service and Supply Risks is rather extensive and available in detail. See Figure 4.2.2-3 and the full-size version at [i.14].

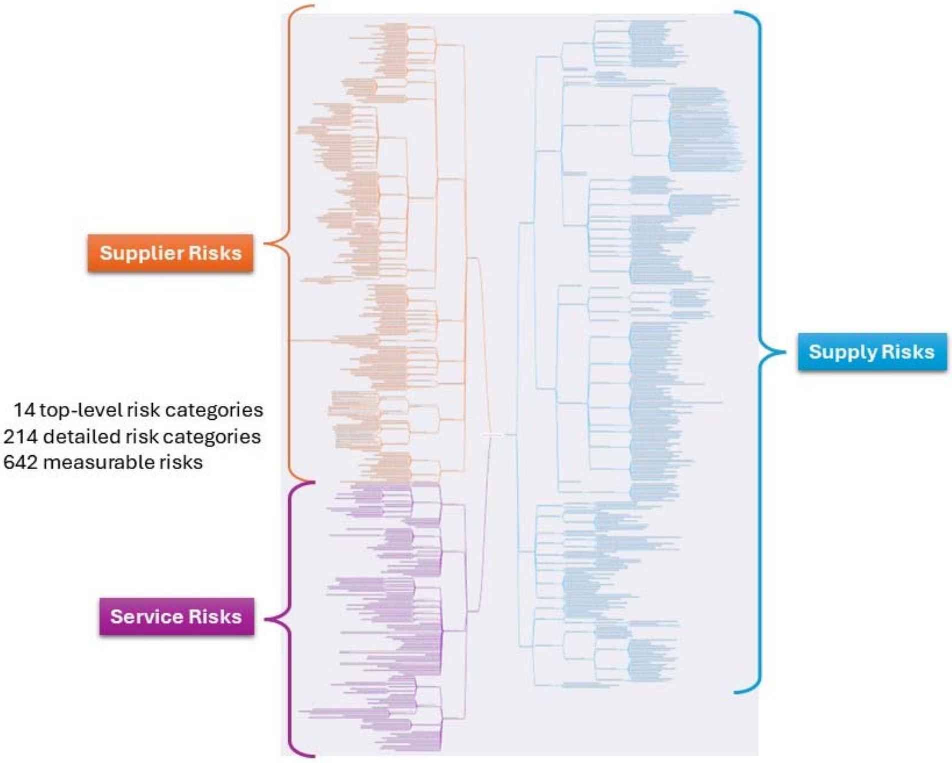


Figure 4.2.2-3: Combined Software Supply Chain, Supplier and Service Risks (Source MITRE [i.14])

IETF - scitt [i.24]. The Supply Chain Integrity, Transparency and Trust (SCITT) WG defines a set of interoperable building blocks that will allow implementers to build integrity and accountability into software supply chain systems to help assure trustworthy operation. For example, a public computer interface system could report its software composition that can then be compared against known software compositions or certifications for such a device thereby giving confidence that the system is running the software expected and has not been modified, either by attack or accident, in the supply chain. SCITT's [i.23] initial work encompasses software use cases and an architecture for trustworthy and transparent digital supply chains.

4.3 Zero trust model frameworks

4.3.1 Government-driven model frameworks to enable Zero Trust

EU. The NIS2 Directive [i.3] includes in its explanatory preamble a statement that "Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles."

France - ANSSI. The Zero Trust model is increasingly attractive because it is promoted as a guarantee of secure access to computing resources in mixed-use contexts.

Germany - BMI. In 2022, the head of the "Cyber and IT Security" department at the Federal Ministry of the Interior (BMI) announced the gradual transition to a zero trust architecture in Germany including creation of transparency for services and products used.

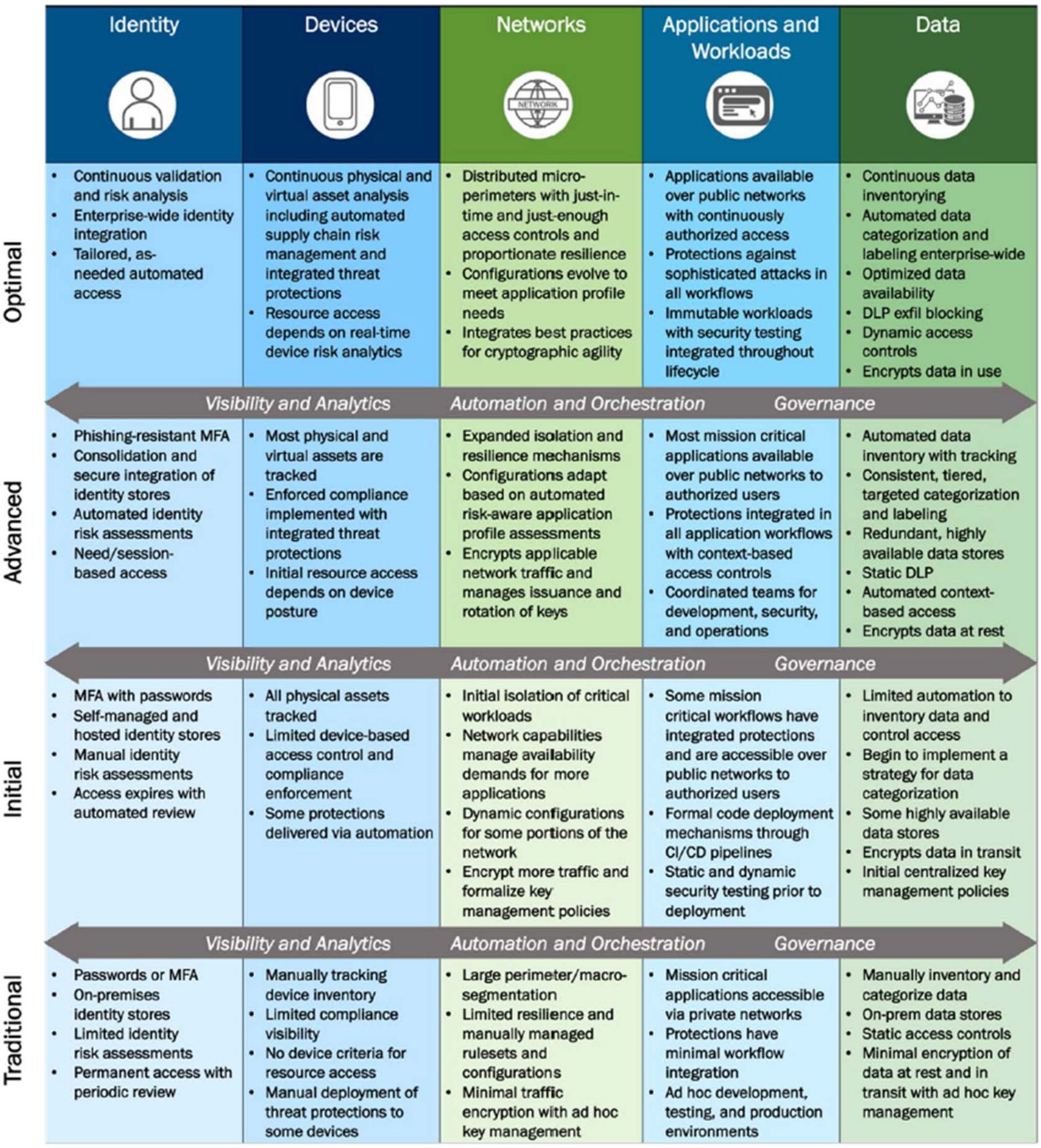
UK - NCSC [i.21]. Zero trust is an architectural approach where inherent trust in the network is removed, the network is assumed hostile and each request is verified based on an access policy. Confidence in the trustworthiness of a request is achieved by building context, which in turn relies upon strong authentication, authorization, device health, and value of the data being accessed. Key concepts include:

1) the network is hostile; and

2) confidence is gained dynamically.

USA - NSA [i.20]. Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses. The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

USA-CISA [i.19]. CISA's Zero Trust Maturity Model (ZTMM) provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. This ZTMM is one of many paths that an organization can take in designing and implementing their transition plan to zero trust architectures in accordance with government mandates which require that agencies develop a plan to implement a Zero Trust Architecture (ZTA). While the ZTMM is specifically tailored for government, all organizations should review and consider adoption of the ZTMM.



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration	Governance	
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration	Governance	
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration	Governance	
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4.3.1-1: ZTMM High-Level Zero Trust Maturity Model Overview (Source [i.19])

4.3.2 Industry-developed model frameworks to enable Zero Trust

3GPP. The Release 18 publication studies some Zero Trust Security principles that can be applied to the 5G System core network, see 3GPP TR 33.894 [i.16]. It analyses potential threats, study necessary security enhancements, and document various decisions related to solutions as to be adopted or not adopted after evaluating the associated risks and the complexity, and includes:

- 3GPP 5GS security scenarios related to the 5G core network that may benefit from Zero Trust principles and identify the associated threats.

- Suitable Zero Trust security mechanisms (i.e. for enabling trust evaluation and ensuring trust) to address the threats identified where potential security risk exists.

- Recommendations for support of additional Zero Trust principles in 5GS security architecture with suitable future normative work directions, where such recommendations may include 3GPP 5G security requirements, technical enhancements, and procedural enhancements.

Cloud Security Alliance [i.17]. "*Enterprise stakeholders must consider the challenges of increased real-time system complexity, the need for new cybersecurity policy, and the strong cultural support that is required to securely operate systems in a complex and hybrid world*". Emerging technology solutions and approaches such as Zero Trust are critical to meeting governmental and sector cybersecurity mandates. The implications of an emerging, rich, and diverse solutions landscape and the challenges to an organization's ability to ultimately deliver a Zero Trust Architecture (ZTA) are necessary. CSA work is directed at improving industry collaboration among key stakeholder groups to accelerate both enterprise leaders' and security practitioners' adoption of Zero Trust into their environments.

NCCoE [i.18]. Zero trust is a cybersecurity strategy that focuses on moving perimeter-based defences from wide, static perimeters to narrow dynamic and risk-based access control for enterprise resources regardless of where they are located. Zero trust access control is based on a number of attributes such as identity and endpoint health. A Zero Trust Architecture (ZTA) is designed for secure access to enterprise resources. Shown in Figure 4.3.2-1 is a high-level, notional architecture of the core components of a ZTA build for a typical IT enterprise and the functional components to support it.

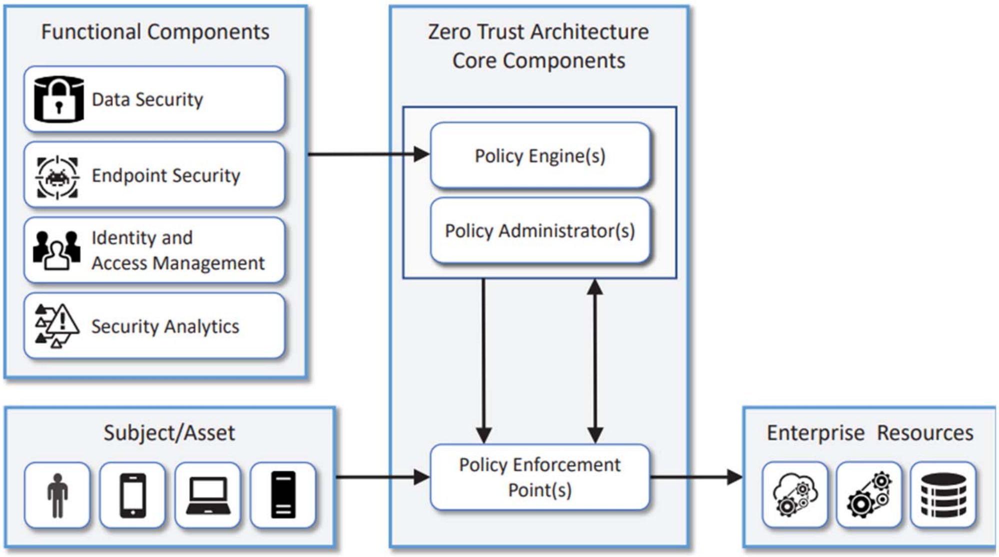


Figure 4.3.2-1: ZTA Notational architecture (Source [i.18])

5 Implementation platforms and measures

5.1 Cyber resiliency platforms and measures

Cyber resiliency it regarded as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Over the past few years, the implementation of this ability has been manifested through a combination of supply chain management practices facilitated though multi-party coordinated vulnerability disclosure and through zero trust maturity model. The two platforms have enabled an understanding and measure of the cybersecurity state of a device, systems and services at designated points in time and contexts in conjunction with Critical Security Controls and facilitation mechanisms. Refer to [i.10], [i.11] and [i.12].

The two predominant cyber resilience platforms and measures are treated in the following clauses.

5.2 Supply chain management platforms and measures

The widespread acceptance of supply chain management platforms, including SBOM, VEX and MITRE's System of Trust together with imposition of mandatory requirements by government authorities and industry sector organizations worldwide has resulted in their widespread use worldwide:

- Generic supply chain risk management [i.13].

- MITRE System of Trust [i.14].
- MITRE enumeration of measurable risks [i.22].
- IETF interoperable building blocks for enhancing supply chain trust [i.23].
- IETF architecture for enhancing supply chain trust and transparency [i.24].
- US national security recommended software supply chain practices [i.25].
- GSMA Software Supply Chain Toolbox [i.28].
- ITU-T Technical Report on software supply chain security threats [i.31].
- UK NCSC Guidelines for AI software supply chain trust [i.26].

5.3 Zero trust platforms and measures

The widespread acceptance of the zero trust model together with imposition of mandatory requirements by government authorities and industry sector organizations worldwide has resulted in their instantiation in service offerings worldwide.

- NIST Special Publication on Zero Trust Architecture [i.15].
- NIST NCCOE guide on implementing a Zero Trust Architecture [i.18].
- 3GPP Technical Report on zero trust security in mobile networks [i.16].
- Cloud Security Alliance guide on Zero Trust Architecture implementations [i.17].
- US CISA specification for a Zero Trust Maturity Model [i.19].
- US NSA guide on implementing a Zero Trust Security Model [i.20].
- UK NCSC design principles for implementing a Zero Trust architecture [i.21].
- US NSA cybersecurity implementation recommendations for Zero Trust [i.27].
- ITU-T Technical Report on guidance for implementing a Zero Trust platform in telecommunication networks [i.30].

Annex A: Bibliography

- ANSSI: "Le modèle Zero Trust".
- BSI: "Bundesinnenministerium: Zero-Trust-Architektur wird angestrebt".
- CISA: "Zero Trust Maturity Model" June 2021, Version 1.0.
- CSA, Circle: "Zero Trust".
- MITRE: "Trusting Our Supply Chains: A Comprehensive Data-Driven Approach".
- NSTAC: "NSTAC Report to the President: Zero Trust and Trusted Identity Management", 23 February 2022.
- On2IT: "NIS2: ON2IT expands its Zero Trust as a Service (ZTaaS) platform with support for compliance".
- European Digital SME Alliance: "Cyber Resilience Act: SME Impact Survey".
- Good Access: "NIS2 to require zero-trust as an essential security measure". https://www.goodaccess.com/blog/nis2-require-zero-trust-essential-security-measure
- ITU Workshop on "Zero Trust and Software Supply Chain Security," Goyang, Republic of Korea, 28 Aug 2024.
- Carnegie Mellon University: "Software Bill of Materials (SBOM) Framework: Informing Risk Reduction".
- Software Engineering Institute: "The SEI SBOM Framework: Informing Third-Party Software Management in Your Supply Chain".
- Carnegie Mellon University: "Designing Vultron: A Protocol for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)".
- TechTarget: "How to conduct a cyber-resilience assessment".
- CSA: "Zero Trust Principles and Guidance for Identity and Access Management (IAM)".
- NCSC, NSA et al.: "Identifying and Mitigating Living Off the Land Techniques".

History

Document history		
V1.1.1	August 2024	Publication