Supply Chain Toolbox

GSMA

June 2025

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to unlock the full power of connectivity so that people, industry and society thrive.

Led by our members, we represent the interests of over 1,100 operators and businesses in the broader ecosystem. The GSMA also unites the industry at world-leading events, such as MWC (in Barcelona, Kigali, Las Vegas and Shanghai) and the M360 Series.

Unlock the benefits of GSMA membership

As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis – as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit:
http://www.gsma.com/membership/

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Contents

Contents

Executive summary

This report is intended for those interested in the security aspects involved in the development or procurement of mobile products and services. The report presents a series of 'tools' that can be used by suppliers to demonstrate their security credentials or by mobile network operators to consider during vendor selection during the procurement stage. The tools in this 'toolbox' include both GSMA services and best practice and wider security considerations, each presented within an example lifecycle. Readers are invited to consider how their own supply chain security practices align to those presented within this document and review any gaps or variances.

A mobile telecom supply chain can be broken down into the components of a network that go together to deliver a resilient operational service. Operational and supporting IT infrastructure networks are composed of a variety of products and services procured from a wide range of suppliers. A full assessment of the supply chain might contain technical compliance and more commercial considerations, such as value-for-money, budget allocation, agreement of commercial terms, invitation to tenders (ITTs), shortlisting, best and final offers (BAFO), supplier due diligence and financial risk. However, the Supply Chain Toolbox focuses solely on the security aspects relating to supplier selection.

The classification of mobile infrastructure as critical national infrastructure in many jurisdictions, and concerns about national security have increased focus on the security posture of network equipment and the providers of it. National government responses vary from restricting use of certain vendors, implementing new defensive regulations and security requirements, through to attempts to broaden existing vendor arrangements via open networking and wider initiatives. A European Union report,[1] *Report on the cybersecurity and resiliency of the EU communications infrastructures and networks*, highlights a range of supply chain risk scenarios including where the network or systems of a supplier (this may also include open-source supply) was attacked to introduce a vulnerability, and how that vulnerability was then exploited when in-service.

The GSMA is committed to building security resilience by providing a range of advice, guidelines, recommendations, working group activities, discussion fora and threat mitigations; some of which are outlined below. It is through these activities that the GSMA makes an ongoing contribution and provides leadership in mobile network security.

GSMA member engagement in GSMA's security activities is straightforward, delivers real-time intelligence value and acts to deliver long-term value through using existing and developing new valuable guidelines, services and recommendations. The best security defences are built in a layered fashion with baseline capabilities supporting other layers of security to build a robust and efficient defence strategy. This layered defence approach is discussed later in the report.

The GSMA Supply Chain Toolbox outlines an example product and service lifecycle as a framework to align a number of guidelines ('tools' in the 'toolbox') to help operators and their suppliers to better understand security and how 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 organised to illustrate tools appropriate before and during procurement on services and products and during their in-life operation. The Toolbox first focuses on product and service selection and finally identifies considerations for products and services *in-life*.

1. https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

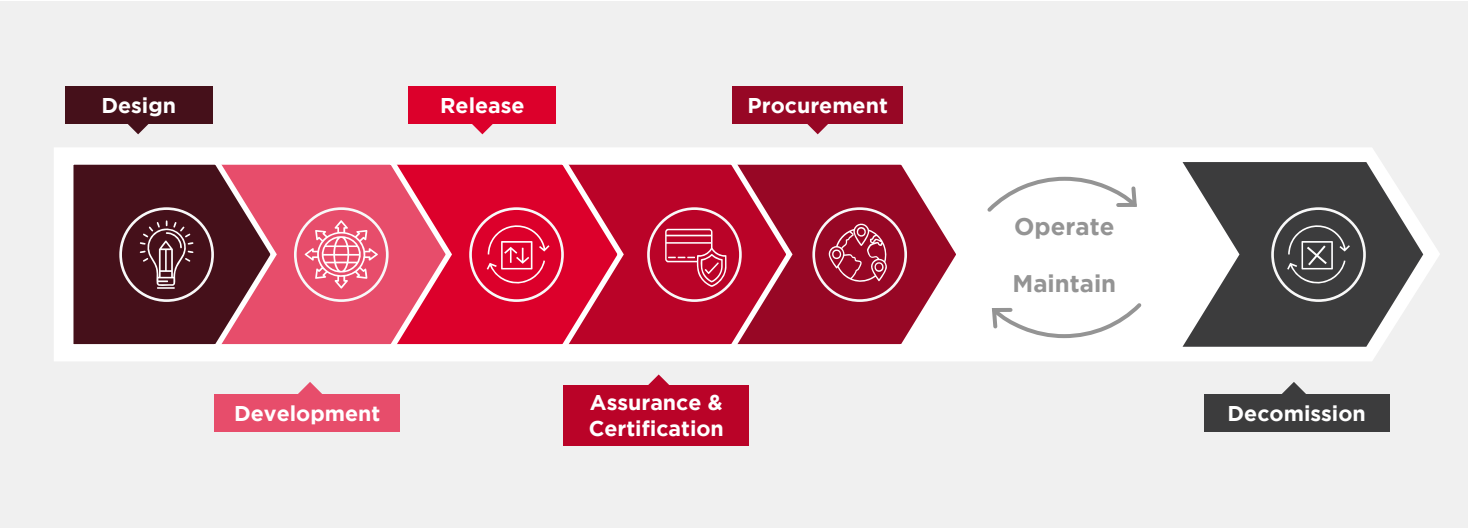
Product and development lifecycle

To understand and strengthen supply chain arrangements, it is important to understand how products and services are developed, built, procured, operated and decommissioned. Supply chain interventions throughout the lifecycle can:

- inform of the strength of development processes
- understand the adequacy of in-built security controls and assurances
- be clear on the security of in-life security maintenance arrangements
- improve the speed of response to mitigate new security vulnerabilities
- ensure decommissioning is undertaken in a controlled and secure manner

The mobile industry has long aimed to deliver robust security arrangements to protect its assets, customers and services. This security objective is delivered through a lifecycle approach starting even before a service goes live. The foundations of security are built through architectural design choices, choosing to adopt solutions utilising internationally recognised standards and shortlisting vendor solutions that already have a strong baseline security level built-in.

A simplified example of a product and service lifecycle is illustrated below. A number of supply chain incidents that have affected live operational networks have their origins in the earlier life cycle stages.[2] The product and service risk owner in the early stages of the lifecycle resides with the vendor / service provider. From procurement, through the operational in-life stages, the operational risk resides with the network operator.



This lifecycle is simplified, as real-world stages are not as linear as illustrated, often involve iterative stages, and can also contain hundreds of products and services that co-exist within a live mobile network. Nonetheless, this lifecycle is presented[3] as a framework on which this report overlays several security best practices that can deliver a stronger and more resilient supply chain.

This report presents a number of security tools that apply to the early lifecycle stages, prior to the procurement stage. This report highlights relevant GSMA-provided services and security frameworks and a wider set of considerations and best practices that are relevant in these stages.

The procurement phase is a vital first step for mobile network operators to select the suppliers they wish to deploy. During procurement, there are a range of approaches that can be undertaken to give confidence in the security of the suppliers under consideration.

The in-life operate / maintain security considerations are often largely dictated by the previous product and service selection. However, this report also points to a range of existing GSMA best practices and services designed to enhance in-life network security.

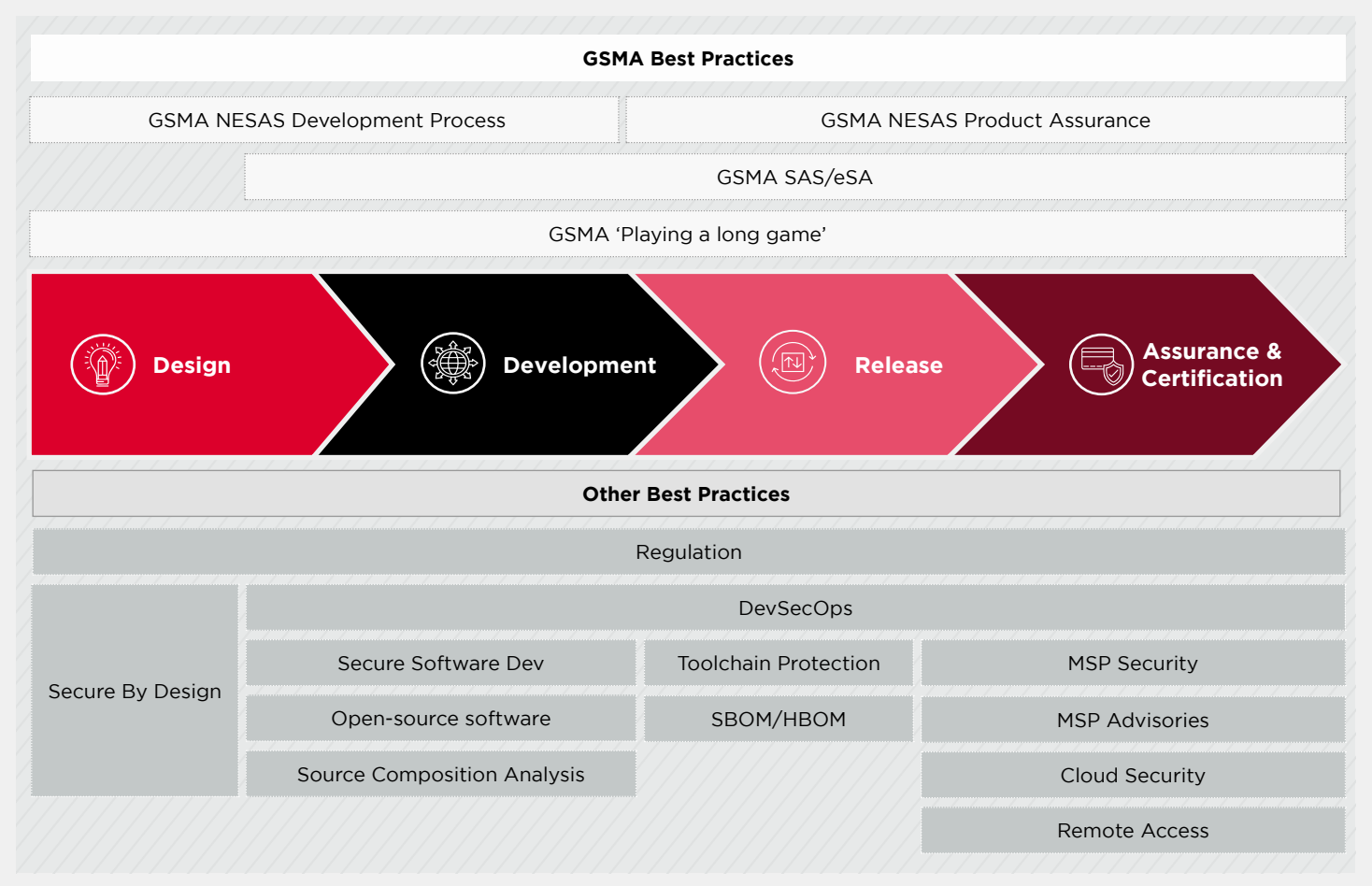
2. For example, the 2021 Solarwinds supply chain attack where an attacker compromised the build platform and installed an implant that injected malicious code into new builds: https://www.solarwinds.com/sa-overview/securityadvisory

3. A fuller description of these lifecycle stages can be found in the GSMA report at https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/security-assurance-andcertification/

Product and service development stages

This section examines some of the best practices that can be deployed in the robust development of secure products and services; the lifecycle stages shown below and described in following sections.

These product and service owners will have their own in-house development and test processes and these can be proven to prospective customers in differing ways including assurance / certification activities, robust code development processes, provision of product documentation such as software and hardware bills of materials, comprehensive release notes, secure arrangements for remote support.



Secure-by-design

A secure-by-design (SBD) software development process is a systematic approach applied throughout the development lifecycle that places security at the centre of product development. SBD applies the process beyond just the design phase where security risks are considered at the requirements, design, implementation, testing, deployment, and maintenance stages. A foundational component of SBD is to actively undertake threat assessments informed by the operating security landscape.[4] In this way, robust security foundations can be established for both products and services. The concept is well established[5] and can form a fundamental part of any development lifecycle. From a supply chain perspective, mobile network operators may wish to consider the benefits of a robust secure-by-design process from their prospective suppliers.

4. E.G see https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2025/
5. https://www.cisa.gov/securebydesign, https://www.ncsc.gov.uk/collection/cyber-security-design-principles & https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

Secure software development

Software code implements product functionality. The code can be proprietary and contain open-source components and may contain commercially supported open-source virtualisation software to allow interfacing between the code and the supporting open hardware or cloud infrastructure. When considering deployment of products that are not assured through the NESAS approach,[6] consideration can be given to examination of the software development processes that are used to build the products. Whilst an in-depth assessment may be difficult, it can be instructive to make an informed assessment of software development approaches. This can form part of the third-party risk assessment process.

The NIST Special Publication 800-218 defines their Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. This SSDF was developed further to the U.S. Presidential Executive Order 14028 and whilst it is intended to address the requirements of the U.S. government in the procurement of more secure software, the principles outlined are broadly applicable to other domains such as telecoms. The topic of secure software development is also discussed in an ENISA study.[7] The study discusses some key elements of software security and provides an overview of some existing approaches and standards while identifying some shortcomings. Open Worldwide Application Security Project (OWASP) aims to provide an effective and measurable way to analyse and improve a secure development lifecycle through its Software Assurance Maturity Model (SAMM).[8] SAFECode made their Framework for Examining the Secure Development Processes of Commercial Technology Providers available.[9] The Enduring Security Framework (ESF) Software Supply Chain Working Panel has suggested practices[10] for developers,[11] suppliers,[12] and customer stakeholders[13] to help ensure a more secure software supply chain. Each (or a mix) of these approaches may be an appropriate framework through which to frame, assess, audit and test a vendor's existing software security practices.

Open-source software

There is significant use of open-source code within many proprietary / closed source code developments. There are strengths and weaknesses to this approach and the topic is developed and discussed more fully in a GSMA Report: *Open Networking & the Security of Open Source Software Deployment*.[14] CISA has released[15] a factsheet that aims to improve the security of open-source software in operational technology and industrial control systems.

6. See later section of this report
7. https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework
8. https://owasp.org/www-project-samm/
9. https://safecode.org/wp-content/uploads/2015/11/SAFECode_Principles_for_Software_Assurance_Assessment.pdf
10. https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF
11. https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
12. https://media.defense.gov/2022/Oct/31/2003105368/-1/-1/0/SECURING_THE_SOFTWARE_SUPPLY_CHAIN_SUPPLIERS.PDF
13. https://media.defense.gov/2022/Nov/17/2003116445/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_CUSTOMER.PDF
14. https://www.gsma.com/security/resources/the-security-of-open-source-software-deployment/
15. https://www.cisa.gov/sites/default/files/2023-10/Fact_Sheet_Improving_OSS_in_OT_ICS_508c.pdf

Software composition analysis

Software composition analysis (SCA) is an increasingly important approach to code assessment. Techniques vary from:

- static code testing
- composition analysis
- fuzz testing
- dynamic application security testing

An earlier GSMA report,[16] *Open Networking & the Security of Open Source Software Deployment* included reference to several organisations active in considering SCA approaches. These included:

- the OWASP Dependency Check[17]
- SAFECODE's Report: Managing Security Risks Inherent in the Use of Third-party Components[18]
- Linux Networking Foundation's OpenChain tool[19]
- Synopsys' SCA tools[20] and the Open-Source Security and Risk Analysis paper[21]
- Whitesource's SCA: *how to choose the right solution*[22] and the Complete Guide to open-source security[23]

From a supply chain perspective, mobile network operators may wish to consider verifying the software code testing that has been undertaken for any potential vendors.

DevSecOps

Operators are moving more towards a 'development, security, operations' (DevSecOps)[24] process that more closely integrate security considerations in the software builds. Depending on the implementation approach, it may be unlikely that operators will have influence over much of the development process. The advantage of the DevSecOps approach is to increase the speed of code deployment into live networks. Traditionally, there were separate 'production' (development) networks and 'live' (operations) networks. This allowed a partitioning of technical risk as development code could be tested away from live networks, thus de-risking new deployments. On a similar topic, 'continuous integration / continuous development' (CI/CD) methodologies have attracted some best practice guidance[25] *Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines*.

Toolchain protection

Toolchain protection and code check-in are important considerations[26] when evaluating a particular tool or software build. If toolchains are insecure, a significant vulnerability is created and should be considered at this early stage. Similarly, it is important to have the ability to protect software / container images taken from a registry /repository so support for this should be designed in. The need to protect the authoritative source for software[27] is critical to preventing the surreptitious introduction of malicious code. This topic is addressed in the Australian Signals Directorate Guidelines for Software Development[28] alongside a range of software development security considerations. From a supply chain perspective, mobile network operators may wish to consider verifying the security robustness of potential vendor toolchains

16. https://www.gsma.com/security/wp-content/uploads/2020/12/Open-Source-Software-Security-Research-Summary-v1.1.pdf
17. https://owasp.org/www-project-dependency-check/ is a Software Composition Analysis (SCA) tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies. It does this by determining if there is a Common Platform Enumeration (CPE) identifier for a given dependency. If found, it will generate a report linking to the associated CVE entries.
18. https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
19. The LF https://www.openchainproject.org/ initiative maintains the industry-standard for the key requirements of a quality open source compliance program. It seeks to make open source license compliance simpler and more consistent
20. https://www.synopsys.com/software-integrity.html
21. https://www.synopsys.com/blogs/software-security/5-open-source-trends-2020-ossra/
22. https://resources.whitesourcesoftware.com/white-papers-datasheets/how-to-choose-an-open-source-management-solution
23. https://resources.whitesourcesoftware.com/white-papers/the-complete-guide-on-open-source-security
24. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsFundamentals.pdf
25. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204D.pdf
26. See pp 14-16 of https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
27. See https://repos.openssf.org/principles-for-package-repository-security
28. https://www.cyber.gov.au/sites/default/files/2023-12/18.%20ISM%20-%20Guidelines%20for%20Software%20Development%20%28December%202023%29.pdf

SBOM and HBOM

Utilising software bills of materials[29] (SBOMs) and hardware bills of materials[30] (HBOMs) can be used as a means to deliver, track and maintain clearer equipment and software supply chains, with additional benefits of tracking licensing and responding faster to new security vulnerabilities.

The maturity of SBOM, in practice, is still evolving. There are several areas where further work will assist in delivering the full potential including differing formats (e.g. SPDX and CycloneDX), suitably addressing intellectual property rights information, false positives and operating at scale.

The composition of the source code is ideally documented in detail to describe how the code works to assist in code maintenance and upgrade by other coders. The code composition can be recorded in a SBOM.[31] The SBOM allows a detailed record of code components, especially re-used code, that can allow much improved support for the code when in-life. For example, should a new code vulnerability be spotted and published (such as common vulnerability exposures (CVEs), then an entity can check whether their code is affected by checking against the SBOM and can take appropriate remedial action (such as applying a patch, disabling the code, changing vendor).

Vulnerability Exploitability eXchange (VEX)[32] has the goal to communicate the exploitability of components with known vulnerabilities linked to the product in which they are deployed. VEX allows software vendors to communicate the exploitability status of vulnerabilities and is an important provision in the beneficial exploitation of SBOMs.

There are a range of approaches to enhance the overall software supply chain. One example is the Supply-chain Levels for Software Artifacts[33] (SLSA) for tracking attestations of the supply chain and software development life cycles. SLSA is a security framework and a checklist of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure. Additionally, the open-source Graph for Understanding Artifact Composition (GUAC)[34] aims to ingest software metadata and map out relationships between software, thus allowing greater insights into the security of the software supply chain. GUAC builds a graph of the relationships between the data, such as SBOMs and vulnerability statements in order to provide information that then can be used to locate and remediate vulnerable dependencies.

From a supply chain perspective, mobile network operators may wish to consider the value of requiring SBOMs / VEX from their vendors in order to better understand the code composition.

29. https://www.gartner.com/en/documents/4893131
30. https://www.cisa.gov/sites/default/files/2023-09/A%20Hardware%20Bill%20of%20Materials%20Framework%20for%20Supply%20Chain%20Risk%20Management%20%28508%29.pdf
31. Types of Software Bill of Materials (SBOM) Documents (cisa.gov)
32. https://cyclonedx.org/capabilities/vex/ and https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex
33. https://slsa.dev/spec/v1.0/
34. https://guac.sh

Regulation

In many countries, MNOs are tasked by regulation to deploy and run, reliable and robust networks. As one element of achieving this, MNOs rely on secure network equipment being provided by their vendors. Thus, for MNOs, it is important to be able to understand the level of security within any specific product provided by their chosen vendors. The following two approaches are considered suitable to achieve this (noting that the GSMA's Network Equipment Security Assurance Scheme [NESAS], as explained in the next section, provides these):

- firstly, assessment of the security related to the product development and lifecycle management processes
- secondly, security evaluation of network equipment products by a competent test laboratory with standardised security tests against an agreed security target

An example of the emerging regulation is the European Commission Cyber Resilience Act (CRA),[35] which defines both horizontal and vertical requirements based on a set of critical product classes for products with digital elements. The Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle. The Act aims to:

- ensure that products with digital elements placed on the EU market have fewer vulnerabilities and that manufacturers remain responsible for cybersecurity throughout a product's life cycle
- improve transparency on security of hardware and software products
- business users and consumers benefit from better protection.

The Act introduces significant responsibilities for the equipment manufacturer:

- ensure cybersecurity is taken into account during planning, design, development, production, delivery, and maintenance
- document all cybersecurity risks
- report actively exploited vulnerabilities and incidents
- ensure that, once sold, vulnerabilities are handled effectively throughout the support period
- provide clear and understandable instructions for the use of products with digital elements
- make security updates available to users for the time the product is expected to be in use

To consider a wider set of service provision, the European Union (EU) has introduced the Networks & Information Systems (NIS2) directive.[36] This directive aims to enhance the security of service offerings within the EU through implementation of national regulations. For those involved in, or in the supply chain for, financial services within Europe, the European Union introduced the Digital Operational Resilience Act (DORA).[37] DORA aims to prevent and de-risk cyber threats and to ensure that financial entities can withstand, respond better to, and recover from, all types of cybersecurity disruptions and threats. Article 1(2) of DORA provides that, in relation to financial entities covered by the NIS 2 Directive and its corresponding national transposition rules, DORA shall be considered a sector-specific Union legal act for the purposes of Article 4 of the NIS 2 Directive.

35. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
36. https://eur-lex.europa.eu/eli/dir/2022/2555
37. https://www.gsma.com/security/resources/the-security-of-open-source-software-deployment/

GSMA NESAS[38]

The GSMA NESAS exists to facilitate improvements in network equipment security levels, across the mobile industry by providing a baseline security assurance. Providing one universal and global security assurance framework that can raise confidence and trust in mobile network equipment.

The purpose of the scheme is to audit and test network equipment vendors, and their products, against a security baseline, so they can demonstrate to network operators (or regulators) that they are conforming to the desired standard. The scheme has been defined by industry experts through GSMA and 3GPP. Therefore, it represents a key pillar in securing the whole ecosystem, including the needs governments, mobile network operators and regulators. NESAS plays only one part in the overall security strategy, testing products and processes at a single point in time. It is important to guarantee that the actual deployed code is actually the same code that was tested through NESAS. Additional layers of security are required to deliver a robust deployment for in-service use. In addition, GSMA's Network Equipment Security Assurance Scheme brings other benefits to equipment vendors and MNOs. Firstly, having one scheme decreases the duplication of work and security testing when serving a variety of markets. Secondly, it increases the transparency and comparability of the products on offer to network operators.

The NESAS approach consists of the following steps:

1. Equipment vendors define and apply secure design, development, implementation, and product maintenance processes.
2. Equipment vendors assess and claim conformance of these processes with the NESAS defined security requirements.
3. Equipment vendors demonstrate these processes to independent auditors.
4. Level of security of network equipment is tested and documented.
5. Tests are conducted by competent and authorised test laboratories against defined security requirements.
6. Documentation can be forwarded to purchasing operators.

GSMA SAS[39]

The Universal Integrated Circuit Card (UICC) in mobile devices, and its applications and data play a fundamental role in ensuring the security of the network, the subscriber's account and related services and transactions. To safeguard the integrity of UICCs, of Embedded UICCs (eUICCs)[40] with remote provisioning capabilities, and of their applications and data, it is essential that the supplier environment and processes that are used to manufacture and/or manage UICCs and eUICCs are secure.

The GSMA's Security Accreditation Scheme (SAS) enables mobile operators, regardless of their resources or experience, to assess the security of their UICC and eUICC suppliers, and of their eUICC subscription management service providers. Two schemes operate under SAS:

- SAS for UICC Production (SAS-UP): This is a well-established scheme through which UICC and eUICC manufacturers subject their production sites and processes to a comprehensive security audit. Successful sites are awarded security accreditation for a period of one year, extending to two further years upon each successful renewal. This scheme has accredited some of the industry's largest suppliers.[41] GSMA also provides advice[42] to its members on how to benefit from SAS-UP.
- SAS for Subscription Management (SAS-SM): To ensure industry confidence in the security of remote provisioning for eUICCs, a related security auditing and accreditation scheme exists for the providers of eUICC subscription management services.

GSMA eUICC Security Assurance

The GSMA eUICC Security Assurance (eSA) scheme[43] is an independent security evaluation for evaluating embedded UICCs (eUICCs) against the provisions of protection profiles for eUICCs. The scheme aims to establish trust for service providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secure against state-of-the-art attacks. The scheme is based on the 'common criteria' methodology, optimised for GSMA-compliant eUICCs.

38. https://www.gsma.com/security/network-equipment-security-assurance-scheme/
39. https://www.gsma.com/security/security-accreditation-scheme/
40. https://www.gsma.com/esim/
41. https://www.gsma.com/security/sas-accredited-sites/
42. https://www.gsma.com/security/wp-content/uploads/2019/06/GuideToUsingSAS-v2.pdf
43. https://www.gsma.com/solutions-and-impact/industry-services/certification-services/gsma-euicc-security-assurance-test-trust-assure/

Playing a long game

A GSMA report,[44] Security Assurance and Certification – playing the long game, examines how today's actions in engaging in industry certification schemes, international standards and developing industry security best practice guidance deliver an enduring long-term benefit.

Given there is sometimes a long in-life equipment usage stage, there is considerable benefit for industry involvement in:

- reaping a longer-term security benefit by actively supporting the development of international standards
- applying and developing industry-developed security best practices through active engagement in GSMA's working groups
- developing coherent vendor arrangements that avoid fragmentation through actively supporting and specifying the use of industry certification schemes such as GSMA's NESAS scheme
- strengthening the collective operational security response through threat intelligence by joining and contributing to GSMA's T-ISAC scheme, and security vulnerability sharing through GSMA's CVD scheme

The relative ease of engagement in these areas means that playing the 'long game' for security can deliver high impact engagements with long-term residual value. By intervening early in the lifecycle, supply chain security benefit can be gained later in that product and service lifecycle when it is deployed in a real network.

Managed service provider security

The security arrangements of any third-party supplier offering or supporting interconnection services are a key focus. Threat actors can use a vulnerable Managed Service Provider (MSP) as an initial access vector to multiple victim networks, with global force-multiplier effects. For example, threat actors successfully compromising an MSP could enable later activity—such as ransomware and cyber espionage—against the MSP as well as across the MSP's customer base.

The variety of significant supply chain incidents and supply chain threats has prompted publication of best practices that aim to mitigate supply chain risks. These are notably in the managed service provider area where there may have been inherent customer / supplier and / or partner trust arrangements rather than explicit and enforced security requirements. ENISA has released[45] a supply chain cybersecurity good practices guide, NIST has released Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,[46] Australia has released[47] a guide to Cyber Supply Chain Risk Management and the UK's National Cyber Security Centre has released a guide.[48] The combination of government regulatory 'push' and the availability of increasingly valuable supply chain guidance 'pull' assist in the production and maintenance of meaningful and in-depth supply chain management plans.

From a supply chain perspective, mobile network operators may wish to consider alignment with these best practice security arrangements for any potential service provider.

44. https://www.gsma.com/security/resources/security-assurance-andcertification/
45. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
46. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
47. https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Cyber%20Supply%20Chain%20Risk%20Management%20%28May%202023%29.pdf
48. https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

MSP advisories

CISA, NSA, FBI and international cyber authorities' cybersecurity advisories have been published to protect managed service providers and customers[49] including:

- prevent initial compromise
- enable/improve monitoring and logging processes
- enforce multifactor authentication (MFA)
- manage internal architecture risks and segregate internal networks
- organisations should apply the principle of least privilege
- deprecate obsolete accounts and infrastructure
- apply updates
- backup systems and data
- develop and exercise incident response and recovery plans
- understand and proactively manage supply chain risk
- promote transparency
- manage account authentication and authorisation

The Australian Signals Directorate (ASD) released a guide,[50] H*ow to Manage Your Security When Engaging a Managed Service Provider.* It contains a number of suggested mitigation strategies including:

- make sure your own network is secure
- get security in the contract
- ensure your contract requires your MSP to maintain a good internal security culture
- control MSP access to your network
- mitigate the impact of stolen or abused credentials
- ensure visibility of MSP actions on your network Plan for a cyber security incident

Also available from the Canadian Centre for Cyber Security is the report, *Cyber Security Considerations For Consumers of Managed Services*.[51] The report covers a range of topics including:

- data security
- legal compliance
- service provider assessments
- access control
- encryption
- incident response
- business continuity and disaster recovery
- supply chain integrity
- exit strategies
- data destruction

From a supply chain perspective, mobile network operators may wish to consider alignment with these best practice security advisories for any potential service provider.

MSP security practices

ASD have released guidance their *Essential Eight*[52] mitigation strategies that aim to enhance defences against malicious activity. The Essential Eight and the accompanying maturity level definitions[53] can form the basis for an assessment of the internal MSP security practices. The Essential Eight are:

- patch applications
- patch operating systems
- multi-factor authentication
- restrict administrative privileges
- application control
- restrict Microsoft Office macros
- user application hardening
- regular backups

From a supply chain perspective, mobile network operators may wish to consider alignment with these best practice security advisories for any potential service provider.

49. https://www.cisa.gov/news-events/news/cisa-nsa-fbi-and-international-cyber-authorities-issue-cybersecurity-advisory
50. https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20How%20to%20Manage%20Your%20Security%20When%20Engaging%20a%20Managed%20Service%20Provider%20%28October%202021%29.pdf
51. https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsm50030-e.pdf
52. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained
53. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Cloud security

5G is designed to be cloud-native and 6G is likely to further rely on cloud and virtualised network infrastructure. As such, virtualised infrastructure is an important and growing component of mobile networks, as demonstrated by:

- the specification for emerging 5G standalone core networks relying on cloud and virtualised infrastructure
- the O-RAN Alliance specifications[54] include the concept of supporting 'O-Cloud' infrastructure.
- mobile Edge Compute (MEC) solutions, which move core functions closer to the network edge, usually entailing the use of virtualised infrastructure

The security of cloud and virtualisation services is particularly important[55] to protect emerging flexible infrastructures and 5G networks (where the architecture has been designed to operate in a virtualised environment). The wide-scale deployment of such virtualised solutions points to the need for a strong control-set to minimise the opportunity for bad actors[56] to cause wide-scale disruption.

Correspondingly, some national telecom security regulations have prioritised increased security controls for virtualised and cloud implementations. The cloud providers are responding to these regulations by releasing public documents[57] that demonstrate how their services meet some of the new government mandates.

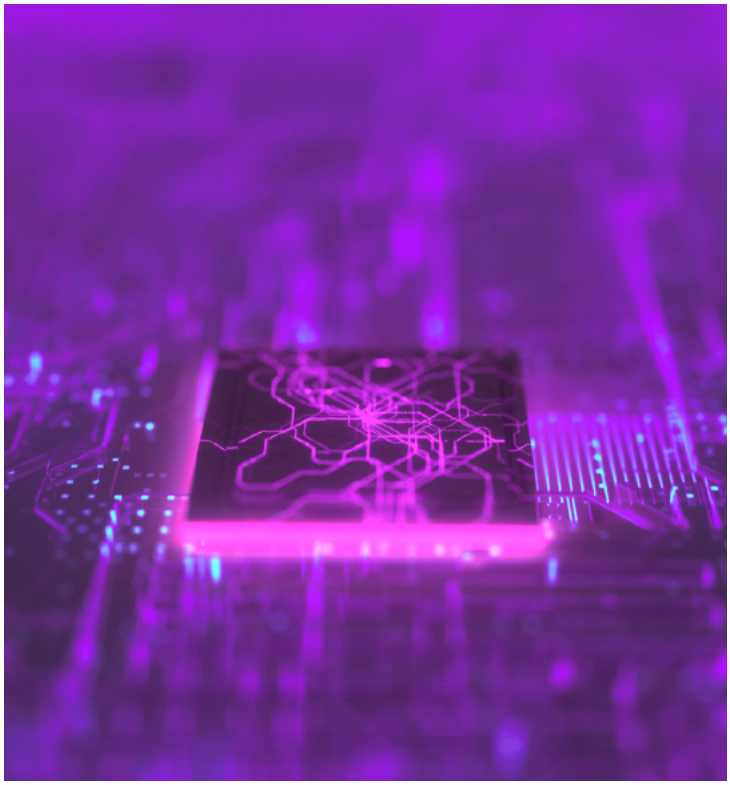
The GSMA has recently updated its Baseline Controls[58] adding further guidance specifically on network function virtualisation and there is ongoing activity within the GSMA's Open Infrastructure Group (closely linked to Linux Networking Foundation's Anuket[59] project). The GSMA document, FS.33, Network Function Virtualisation (NFV) Threats Analysis,[60] provides a detailed view of identified threats and guidance on appropriate countermeasures. The security of managed cloud services is a particularly important topic as cloud services are increasingly deployed to support 5G and other telecoms infrastructure and services. The UK's National Cyber Security Centre has released information[61] in *Cloud Security Guidance*.

Remote access

In order to perform their contracted activities, an MSP must administer their systems and services and without proper controls, this high level of privileged access can leave a system vulnerable to attack.

It is important to identify which systems each MSP can access and what the secure access mechanisms are. These accesses should only allow activities that are within the contracted scope of service provider activity. Segmentation (to limit the scope for lateral movement), least privilege (to decrease the impact a malicious access account may have), use of secure 'jump' boxes, use of dedicated workstations, multi-factor authentication, attributable accounts and' just in time' principles and limited duration access for privileged accounts can all be effective controls.

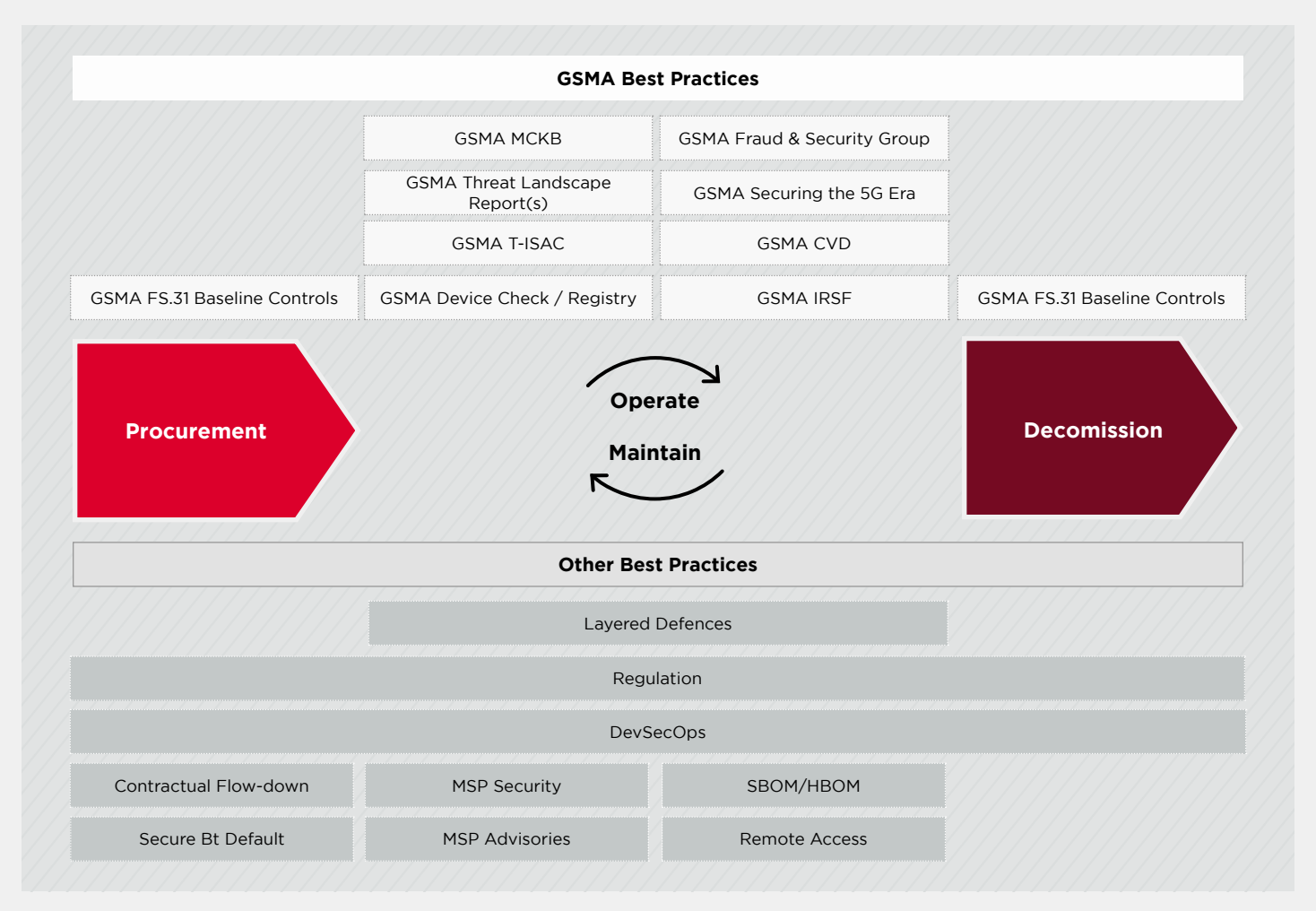
The secure separation of privileged access workstations used by systems administrators is a key area of supply chain security. This topic is discussed in detail in a UK Code of Practice.[62] From a supply chain perspective, mobile network operators may wish to consider alignment with these best practice security advisories for any potential cloud service provider.



54. O-RAN Specifications - https://www.o-ran.org/specifications - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120531/E02781980_Telecommunications_Security_CoP_Accessible.pdf
55. According to CrowdStrike, Cloud environment intrusions increased by 75% YoY, see https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf
56. https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
57. E.g. https://d1.awsstatic.com/whitepapers/compliance/Considerations_on_the_UK_Telecommunications_Security_Act.pdf and https://docs.aws.amazon.com/pdfs/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.pdf
58. https://www.gsma.com/security/resources/fs-31-gsma-baseline-security-controls/
59. https://lfnetworking.org/anuket-orinoco-released/
60. A GSMA member-only document
61. https://www.ncsc.gov.uk/collection/cloud
62. Section 2.26 – 2.30 of

Lifecycle stages from procurement, through in-life and to decommission

The following sections present some tools for both deployed products and enabling MSP services including GSMA advice and services and an additional set of considerations. The diagram below summarises the tools outlined in the 'procurement' lifecycle phase, the 'in-life operate / maintain lifecycle' phase and the 'decommission' phase.



Procurement

Product vendors seek to deploy their solutions in a global market to maximise efficiencies and the market opportunity. In turn, mobile network operators seek to access the widest pool of viable global vendors to maximise competition in supply and access the most innovative products. The availability of equipment developed to internationally recognised technical standards enable the successful inter-working of multi-vendor choices.

Implementing the supply arrangement involves agreeing contractual arrangements between the MNO and the product vendor. These contractual arrangements can clarify the understanding of the supply chain, help in investigations of security incidents and in testing security controls. The flow down on contractual security requirements ensures the vendor(s) take appropriate measures to identify the risks of security compromises, have robust internal security measures and monitoring systems in place to ensure that all network connections and data sharing are managed securely. This flow down would seek to place the same security requirements on sub-suppliers and component providers. Regular audits of the data handling of intermediaries can be established.

NIST cybersecurity risk management best practices for systems and organizations[63] (NIST SP 800-161r1) establishes a comprehensive approach and illustrates the potential for reduced visibility and control with increasing depth of the supply chain.

Threat actors can use a vulnerable MSP as an initial access vector to multiple victim networks, with globally cascading effects. For example, threat actors successfully compromising an MSP could enable follow-on activity—such as ransomware and cyber espionage—against the MSP as well as across the MSP's customer base. There are a range of mitigating controls that can be established to respond to this.

GSMA FS.31 Baseline Security Controls

GSMA document FS.31 Baseline Controls[64] provides a comprehensive set of baseline security controls to help operators understand and establish a strong security posture, helping to improve network security and resilience. It contains a wide range of best practice including procurement, network function and infrastructure and decommissioning advice.

63. https://csrc.nist.gov/pubs/sp/800/161/r1/final
64. https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls

Contractual flow-down of security requirements

Implementing a supply arrangement involves agreeing contractual arrangements between the MNO and the MSP.

These contractual arrangements[65] can clarify the understanding of the supply chain, help in investigations of security incidents and in testing security controls. The flow down on contractual security requirements ensures the MSP(s), including support services provided by mainstream product vendors, take appropriate measures to identify the risks of security compromises, have robust internal security measures and monitoring systems in place to ensure that all network connections and data sharing is managed securely.

Every contractual arrangement should clearly identify the detail of customer personal data being handled by the MSP. Service design controls are implemented to minimise the amount of customer personal data shared for any given external service connection. Regular audits of the data handling of intermediaries can be established.

Secure-by-default

Computing platforms and enabling software contain vulnerabilities that can be exploited for malicious purposes. 'Secure-by-default'[66] means products are delivered in a resilient, 'hardened', configuration against likely exploitation techniques without additional steps to secure them. In this way, the initial deployments have a security baseline on which to layer additional controls. Examples of secure-by-default security measures include:

- eliminate default passwords: requiring administrators to set a strong password during installation and configuration
- disabling known unused network ports: to reduce the attack surface
- enabling secure connection protocols are automatically enabled automatically to protect data in transit from initial deployment
- the build and configuration include up to date patches and code updates without the need for additional provisioning
- secure logging: provides high-quality audit logs to customers at no extra charge
- software authorisation profile: manufacturers should include a visible warning that notifies customers of an increased risk if they deviate from the recommended profile authorisation
- track and reduce 'hardening guide' size: reduce the size of 'hardening guides' produced for products and strive to ensure that the size shrinks over time as new versions of the software are released

Defining secure-by-default requirements within the procurement and delivery phases can build an initial security baseline on which to build fewer additional layered security measures.

65. For example, Section 6.2 of https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120531/E02781980_Telecommunications_Security_CoP_Accessible.pdf
66. https://www.ncsc.gov.uk/information/secure-default & https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

In-life product and service operation

The in-life operate / maintain lifecycle phase enables the deployment, test, roll-out and full-scale use of products and services (developed through the preceding network product lifecycle) to consumers. The duration of this phase varies but supply contracts and capital investments may typically assume 5 -10 year lifetime with review milestones (that can result in the asset lifetime being extended well beyond the original planned obsolescence). Managed service provision of support, remote software / control arrangements and service level agreements (SLAs) are important differentiators. Supply chain interventions due to new governmental legislation or policy stances can drive significant costs if a 'rip and replace' vendor change is enforced.[67]

5G was designed to utilise virtualised / cloud infrastructure, the security of which is vital to the security of the 5G virtualised network functions. In this arrangement, security of software and its associated updates are vital to consider. Operators are moving more towards Development, Security, Operations (DevSecOps) processes that more closely integrate security considerations in the software builds. The advantage of this approach is to increase the speed of code deployment into live networks. As development and operations become more closely linked it allows a faster cycle time of code development and deployment and the potential to deploy smaller incremental code changes. Adopting the right assurance and certification scheme, can support in-life patching and avoid full re-certification of software products.

Operate / maintain can incorporate a range of security practices to augment baseline security including:

- implementing least privilege controls
- supporting role-based access control
- implementing vulnerability management programmes and engaging in the GSMA CVD scheme
- security incident and event management
- tracking and responding to threat intelligence and by sharing to protect the wider ecosystem through GSMA's T-ISAC service.
- undertaking red team exercises to better understand the tactics of advanced persistent threat actors and attack vectors

Typically, the vendor will be required to provide support for the deployed product solution during in-service operation which will include maintenance, deployment of bug fixes and patches, system updates and functional upgrades as well as providing support on incidents that may affect normal operation or compromise security. This may be due to a bug or flaw in the design or to a newly discovered vulnerability. Any changes to the system must follow approved procedures to ensure that integrity and security are maintained. In particular, this will require security testing at a component level and end to end.

GSMA provides a range of security advice, best practices and services that aim to enhance the security posture of deployed mobile networks, and these are described in the following sections.

Fraud and security working group[68]

GSMA document FS.31 Baseline Controls provides a comprehensive set of baseline security controls to help operators understand and establish a strong security posture, helping to improve network security and resilience. It contains a wide range of best practice including procurement, network function and infrastructure and decommissioning advice.

Mobile cybersecurity knowledgebase

As mobile operators around the globe introduce and launch 5G systems while maintaining earlier generation mobile technologies, communications networks will face new security threats and challenges. Understanding, mapping and mitigating these existing and upcoming security threats in an objective, speedy and effective manner has become essential.

To help operators and others in the mobile ecosystem, the GSMA has conducted a comprehensive threat analysis involving industry experts from across the ecosystem including MNOs, vendors, service providers, and regulators, as well as drawing on input from public sources such as 3GPP, ENISA and NIST, and mapped these threats to appropriate and effective security controls.

67. https://www.lightreading.com/5g-and-beyond/replacing-huaweis-80000-5g-antennas-would-cost-germany-billions/d/d-id/783837
68. https://www.gsma.com/aboutus/workinggroups/fraud-security-group

The GSMA has collated this analysis into a mobile cybersecurity knowledge base to provide useful guidance on a range of mobile security risks and mitigation measures. The knowledge base aims to make available to GSMA members the combined knowledge of the mobile ecosystem to increase trust in mobile networks and make the interconnected world as secure as possible. Over time, the knowledge base will be enhanced and extended to respond to the evolving cybersecurity threat landscape.

The mobile cybersecurity knowledge base is an industry effort that composes a set of tools to address threats in the mobile threat landscape and is designed to help key stakeholders (such as MNOs, equipment vendors, regulators, application developers and service providers) understand the security threats posed in a systematic and objective fashion. It provides essential insights for the stakeholders' risk management strategy as well as guidance covering best practices and risk mitigation measures.

The knowledge base facilitates and encourages collaboration to protect networks and services against disruption and unauthorised access as well as the prevention and mitigation of risks. The knowledge base will help to enhance mobile security competencies and capabilities and will strengthen the work of carriers, enterprises, oversight agencies and regulators. At an operational level, the knowledge base offers clear instructions for taking step-by-step actions to build security assurance while considering the entire risk spectrum of mobile end-to-end networks.

Access the GSMA Mobile Cybersecurity knowledge Base

Securing the 5G era[69]

As 5G usage gathers pace in both consumer and enterprise settings, its benefits will spread across the global economy. 5G mobile connectivity is expected to add nearly $1 trillion to the global economy by 2030, with almost half of this coming from new enterprise services and apps, across sectors including finance, healthcare, and education.

5G aims to deliver:

- enhanced mobile broadband
- massive machine-type communications
- ultra-reliable and low-latency communications

The purpose is to be faster, more reliable and manage the scale of devices predicted for the Mobile Internet of Things (MIoT). Enabling the digital transformation of our society, business processes and manufacturing.

To enable this, 5G will deliver multi-network slicing, multi-level services and multi-connectivity network capabilities. To allow the required flexibility, agility and economies of scale these technologies will be delivered via virtual and containerised environments.

This is a revolutionary way of working for the industry.

5G has designed in security controls to address many of the threats faced in today's 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection, and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels.

GSMA provides a range of 5G security advice covering several topic areas including:

- secure-by-design
- 5G deployment models
- subscriber and device protection
- network protection
- technologies leveraged by 5G
- legacy generations
- GSMA 5G security activities
- LTE to 5G comparison

GSMA Mobile Telecommunications Security Threat Landscape

The GSMA's Mobile Telecommunications Security Landscape report[70] focuses on security threats that the GSMA has been tracking both from public sources and from within the GSMA's membership. The report is updated annually and provides a current view of security priorities viewed from the mobile industry.

69. https://www.gsma.com/security/securing-the-5g-era/
70. https://www.gsma.com/security/publications/

GSMA telecommunications ISAC[71]

The GSMA Telecommunication Information Sharing and Analysis Center (T-ISAC) is the central hub of information sharing for the Telecommunication Industry. Information sharing is essential for the protection of the mobile ecosystem, and the advancement of cybersecurity for the telecommunication sector. The information sharing can occur in near-real time through sharing active indicators of compromise (IoCs) as well as sharing best practices for threat detection and mitigation.

As cyber-attacks continue to increase in sophistication and volume, the GSMA T-ISAC is evolving and advancing its services. If you are a GSMA member, you can join T-ISAC and get involved in our upcoming activities. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collates and disseminates information on security incidents within the mobile community – in a trusted and anonymised way.

GSMA Co-ordinated Vulnerability Disclosure (CVD)[73]

GSMA regards the security of mobile network infrastructure and customer equipment such as devices, as essential to the provision of secure and trustworthy services by its members. The GSMA CVD programme gives security researchers a route to disclose a vulnerability impacting the mobile ecosystem meaning the impact can be mitigated before it enters the public domain.

GSMA works with mobile operators, suppliers and standards bodies to develop fixes and mitigating actions to protect customers' security and trust in the mobile communications industry. GSMA encourages disclosure of security research which enhances security levels and better protects assets and customers, and our Coordinated Vulnerability Disclosure programme is designed to support the reporting and remediation of security vulnerabilities at industry level.

GSMA International Revenue Share Fraud (IRSF) Prevention[73]

IRSF costs the industry billions of dollars every year since fraudsters are difficult to identify and most fraud solutions are about detection after the event, rather than prevention. Fraudsters artificially inflate SMS and voice traffic to International Premium Rate Numbers (IPRNs) so they can generate revenue from it, called IRSF.

The GSMA IRSF Prevention service is an important development in telecom fraud countermeasures because it gives you the data you need to intercept an attack before it happens – through large-scale coverage with real-time data. So, you can stop revenue loss before it starts.

GSMA Device Registry[74]

GSMA operates a global registry on behalf of the mobile industry which enables the reporting of lost/stolen and fraudulent devices to help prevent crime, by blocking their sale or use on mobile networks. Mobile network operators and device owners flag the status of these devices, so others can avoid them. For example, if the device is reported stolen, we share the information and recommend the device is blocked from network access and not bought, sold, repaired, insured or used in any way – then potentially return it to the rightful owner. There is a range of use cases as to why devices are flagged using their International Mobile Equipment Identifiers (IMEI). Besides lost/stolen and fraudulently obtained, other common reason is that the device is faulty/broken or subject to an ownership or financial claim, such as when it's in transit, not covered by insurance, in an inventory or being repaired.

Recognising that many network operators are resistant to device blocking, greater participation of device manufacturers and OS developers in utilising block list data to deny service to stolen devices could reduce the existing reliance on network operators to take action. This has the potential to significantly help prevent stolen devices from operating in countries where Device Registry use is poor or non-existent.

71. https://www.gsma.com/security/t-isac/
72. https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
73. https://www.gsma.com/services/fraudsecurity/
74. https://www.gsma.com/services/deviceregistry/

GSMA Device Check[75]

Through GSMA Device Check™ operators can find out instantly whether a device has been reported through the registry of device status. Organisations need to protect themselves against the risk of handling flagged devices which can damage reputations and impact operational margins.

GSMA Device Check™ provides 10+ years of a device's history as well as the device model information and capabilities. Businesses that trade or insure devices can not only find out if they're subject to blocking, but also if constrained by an ownership or financial claim. These are usually the points in the lifecycle of a device when it is more vulnerable or at risk – such as when it is in transit, not covered by insurance, in an inventory or being repaired.

Other in-life considerations

The vendor must be able to provide notification of newly discovered vulnerabilities, data breaches or other security breaches and provide a clear and timely process for resolving issues and providing patches.

- Data breaches may also be subject to local regulations which require the data owner (typically the operator) to notify the regulator of such breaches within a defined period – the vendor will typically need to support this requirement. Failure to report the breach within a timely manner may increase the fines and penalties faced by the operator.
- Where patches for vulnerabilities within software components have been issued, these should be deployed as soon as possible to minimise the risk of exploitation.
- This should also include any people or process errors (e.g. incorrect configuration) that lead to any system compromise, security vulnerability or breach.

A security incident is any intentional or unintentional damage, theft, or unauthorised access that has an impact on the security of an organisation's systems or services. Incidents can impact the confidentiality, availability and integrity of a service, causing unplanned service interruptions. The vendor or third party must be able to support the operator's incident management process and be able to provide solutions and / or remedial action in a timely manner. From a supply chain perspective this might be managed through a series of Service Level Agreements (SLAs) which might be reflected in a maintenance contract.

The Australian Signals Directorate have released their own guidance[76] *Strategies to Mitigate Cyber Security Incidents* and there is a useful discussion[77] in the Canadian Centre for Cybersecurity's Cyber Security Considerations For Consumers of Managed Services.

Any changes to components within the solution whether hardware, software (applications, functions, operating system, container, hypervisor, etc.) or configuration changes should be tested before being deployed in the live environment.

The vendor (or an approved third party) should perform regular testing of the operational solution (in a staging /test environment) to identify any weaknesses in the solution as a result of the latest security / threat insights and to isolate any other issues (e.g. relating to non-optimal configuration).

Decommission

Decommission / system closure terminates equipment and service usage and involves decommissioning, data deletion, system wiping and environmentally secure equipment disposal. Closure can be driven by a number of factors including equipment obsolescence, vendor ban, service closure (e.g., 3G) and lack of support. GSMA document FS.31 Baseline Controls provides a comprehensive set of baseline security controls to help operators understand and establish a strong security posture, helping to improve network security and resilience. It contains a wide range of best practice including procurement, network function and infrastructure and decommissioning advice.

75. https://www.gsma.com/services/tac/about-device-check/
76. https://www.cyber.gov.au/sites/default/files/2023-03/PROTECT%20-%20Strategies%20to%20Mitigate%20Cyber%20Security%20Incidents%20%28February%202017%29.pdf
77. E.g. as discussed in s2.6 of https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsm50030-e.pdf

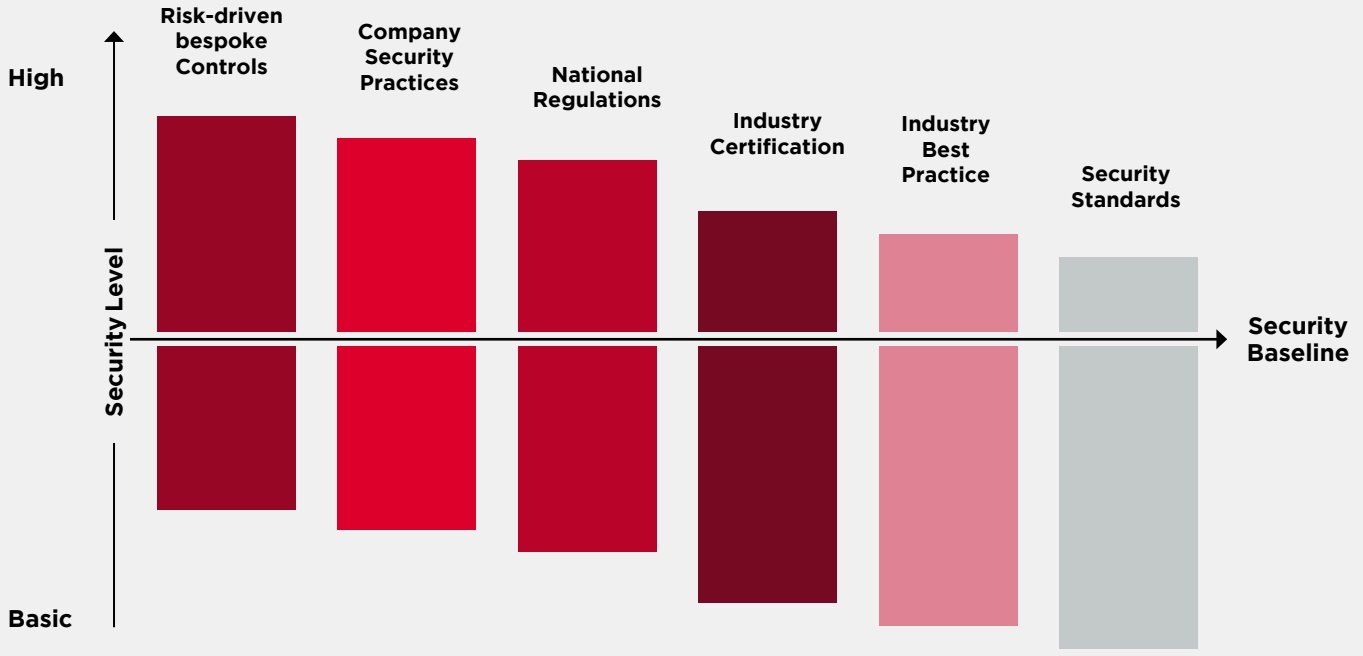
Layered defences

A single or basic security defence can only do so much to protect against attacks, whereas multi-layer defences can work in concert to provide a much more effective defence. In the US, T-Mobile, for example, has explained[78] how layered defences helped it defend against a significant attack.

A holistic and efficient security strategy may be composed of multiple layers as shown below. The combination of security controls taken from each layer build to deliver a bespoke security solution for each operator. Efficient and cost-effective security approaches can be delivered by matching security controls to the threat model, understanding the security benefits built-in by lower level and existing security controls and by customising the security decisions in the higher-level security levels. Areas showing co-incident requirements demonstrate a potential duplication meaning it might be possible to remove duplicate controls. There are initiatives[79] to assist operators in mapping the variety of security controls to understand efficient security risk coverage. Efficient coverage can deliver an effective security design in a cost-effective manner.

The underlying security approaches can act together to provide a baseline security level on which to build a security strategy.

The underlying security approaches can act together to provide a baseline security level on which to build a security strategy.



78. https://www.t-mobile.com/news/un-carrier/update-cyberattacks-targeting-us-wireless-companies
79. E.g. https://www.cisecurity.org/controls/cis-controls-navigator

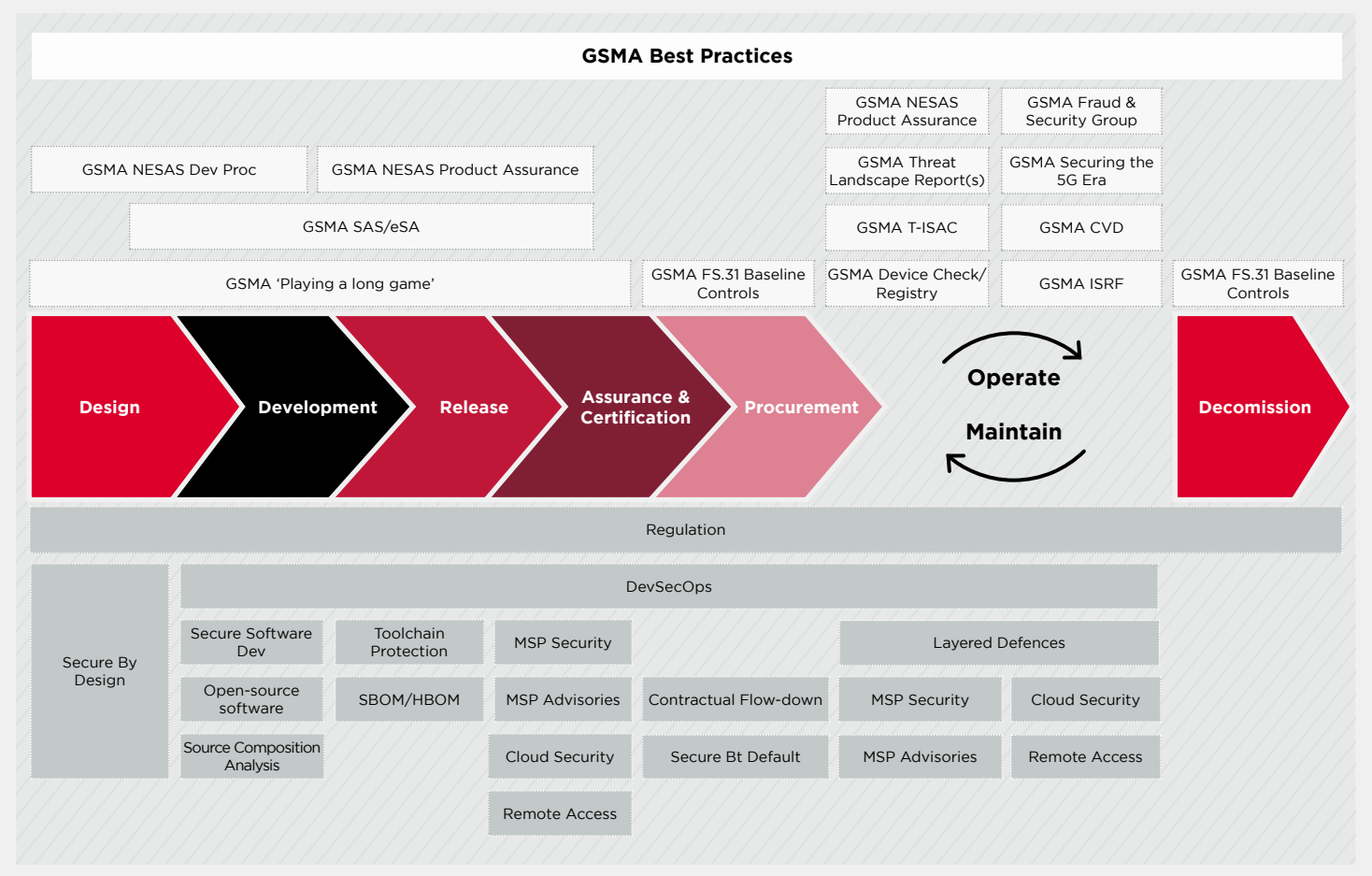
Final thoughts

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 organised to illustrate tools appropriate before and during procurement on services and products and during their in-life operation.

Allied to this, the GSMA's Mobile Telecommunications Security Landscape report[80] has also described the emerging security context and explored many of the more forward-looking security topics and consequences. By considering this context, efficient and strategic security investments can be made that complement the shorter-term security necessities.

Readers are invited to consider how their own supply chain security practices align to those presented within this document and review any gaps or variances.

To get in touch, or to get more closely involved, please email **security@gsma.com**.



80. https://www.gsma.com/security/publications/

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK