Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

009 – Supply Chain Security v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services. They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group Convened on the 23rd, 24th and 25th of June 2020 to discuss matters concerning supply chain security. The group heard from experts in the field of supply chain security and held focussed discussions on the risks, challenges and best practices associated with supply chain security as it pertains to electronic communications networks. ECSM 009 –Supply Chain Security has been developed by the NCSC informed by those meetings.

3 Scope

The ECSMs are applicable to all undertakings providing public Electronic Communications Networks and publicly available Electronic Communications Services.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
ENISA	Technical Guideline on Security Measures under the EECC
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems —

	Requirements
ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls
ISO/IEC 27036:2014	Information technology — Security techniques — Information security for supplier relationships
NIST	Framework for Improving Critical Infrastructure Cybersecurity v1.1
NIST SP 800-100	Information Security Handbook: A Guide for Managers
NIST SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations

30

31 # 5 Definitions, Symbols and Abbreviations

32 ## 5.1 Definitions

Term	Meaning
EU 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020
EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU Member States on 09th October 2019
Hardening	The process of securing a system by reducing its surface of vulnerability, reducing available means of attack. This typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling

	or removal of unnecessary service.
Managed service provider (MSP)	A third-party that helps to run or administrate a network.
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
Network equipment	Software or hardware component of the operator's network that transmits or receives data or provides supporting services to components of the operator's network that transmit or receive data. Includes both virtual machines and physical hardware.
Privileged / Administrative access	An access to network equipment where greater capabilities are granted than a regular user. Accounts granted privileged access can be used to perform elevated security relevant functions including modifying configurations, changing security controls, creating new accounts with equal or greater privilege or allowing full control of network equipment. ..
Privileged user / Administrator	A person who is granted Privileged Access, through their role, access and credentials, or through any other means.
Supply chain	A system of organisations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer

5.2 Symbols

Nil

5.3 Abbreviations

Term	Meaning
3GPP	Third Generation Partnership Project
3PA	Third Party Administrators
CNI	Critical National Infrastructure
ComReg	The Commission for Communications Regulation
DECC	The Department of Environment, Climate and Communications
ECSM	Electronic Communications Security Measures
GSMA	GSM Association
MNO	Mobile Network Operator
MSP	Managed Service Providers
NCSC	National Cyber Security Centre
NESAS	Network Equipment Security Assurance Scheme

6 Overview of Risk

6.1 Dependence

Due to a series of mergers of major telecommunications equipment vendors, the current global marketplace has come to be dominated by a very small number of equipment vendors. This fact, coupled with the challenges associated with interoperability, has resulted in some operators becoming dependent on individual equipment suppliers for access to critical network equipment and the functioning of large parts of their networks. Switching vendors, particularly in the Radio Access Network needs to be managed over time and can be an expensive and complex process.

This dependence carries with it a number of risks. For example, were a systemic vulnerability to be discovered in a supplier's product, a large portion the operator's network may be affected causing widespread disruption and curtailing the operator's ability to provide critical network services. In addition, the operator could experience difficulty in accessing key network equipment, components or spare parts, or be denied access to critical software updates or patching, due to supply disruptions. These could come about for a number of reasons, such as the financial failure of a supplier or the inability of a supplier to access key technology or materials, for example due to a supplier being subject to international trade sanctions.

This scenario was highlighted in the EU risk assessment[1]:

> *"**Dependency**: A mobile network operator sources a large amount of its sensitive network components or services from a single supplier. The availability of equipment and/or updates from this supplier is subsequently drastically reduced, due to a failure by the supplier to supply (e.g. due to trade sanctions by a third State or to other commercial circumstances). In consequence, the quality of a supplier's equipment decreases due to priority given to guaranteeing supply over improvements in product security."*

In a case where all network operators in Ireland become dependent on a single supplier these risks could manifest as national level risks. In order to mitigate these risks, it is important that operators have robust Supply Chain Risk Management processes. The concept of network diversity is further discussed in ECSM 010 – Diversity, Resilience & Continuity.

[1] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

6.2 Equipment Quality

Electronic Communications networks may be compromised through vulnerabilities in their supplier's network equipment. These vulnerabilities can be introduced unintentionally through poor coding practices, or intentionally for malicious reasons. Supply chain compromises take advantage of the trusted relationship between vendors and their customers. The SolarWinds[2] (2020) compromise and NotPetya[3](2017) ransomware attack are two well known examples of widespread supply chain compromises. This compromise could occur either through the supplier cooperating with a state actor, or unwittingly, through a compromise of their systems.

These scenarios are highlighted in the EU-wide risk assessment:

> *"**Low product quality:** Espionage by state or state-backed actors using malware to abuse poor quality network components or unintentional vulnerabilities affecting sensitive elements in the core network, such as Network Virtualisation Functions."*
>
> *"**State interference through 5G supply chain**: a hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities."*

Comprehensive pre-deployment lab testing of network equipment by operators or independent third parties can reduce, but not eliminate, the risks associated low quality equipment. There are ongoing efforts to improve and assure the security of network equipment such as GSMA's Network Equipment Security Assurance Scheme (NESAS) and 3GPP's defining of Security Assurance Specifications (SCAS). In January 2021 the European Commission requested that ENISA proceed with the preparation for a new candidate cybersecurity certification scheme for 5G.[4] This specifically requests that ENISA examine GSMA's NESAS and eUICC schemes as the basis of certification. There will be a two phase approach, with the scheme initially being adapted 'as-is', followed by a risk assessment to identify any gaps in order to strengthen the scheme.

[2] https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[3] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[4] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-commission-requests-eu-cybersecurity-agency-develop-certification

The ECSMs aim to reduce the risks associated with compromise of suppliers by passing down robust security requirements from operators to suppliers. All of these measures will enhance the assurance of the security of network equipment. However, the most important driver to increase security and quality standards will be the demands of network operators.

6.3 Third Party Network Access

Operators often provide administrative access to Managed Service Providers (MSPs) as part of a managed service contract or to an equipment vendor as part of a third-line support function. Due to their nature, these entities gain access to multiple electronic communications networks. This means that a single set of administrators, and administrative systems, can negatively impact multiple networks, making them particularly attractive to attackers. Should a third party system be exploited, or have a malicious insider, multiple networks could be exploited or disrupted simultaneously.

Operation Cloud Hopper (2016) was a successful compromise of a number of global MSPs by the hacking group known as APT10 which highlighted the risks associated with a compromised third party.[5] The attackers leveraged the trusted connections between the MSPs and the victims in order to exfiltrate huge volumes of sensitive data. The indirect approach of reaching many through only a few targets demonstrates a high-profile example of a supply chain attack demonstrating the advanced capabilities of well-resourced attackers.

[5] https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

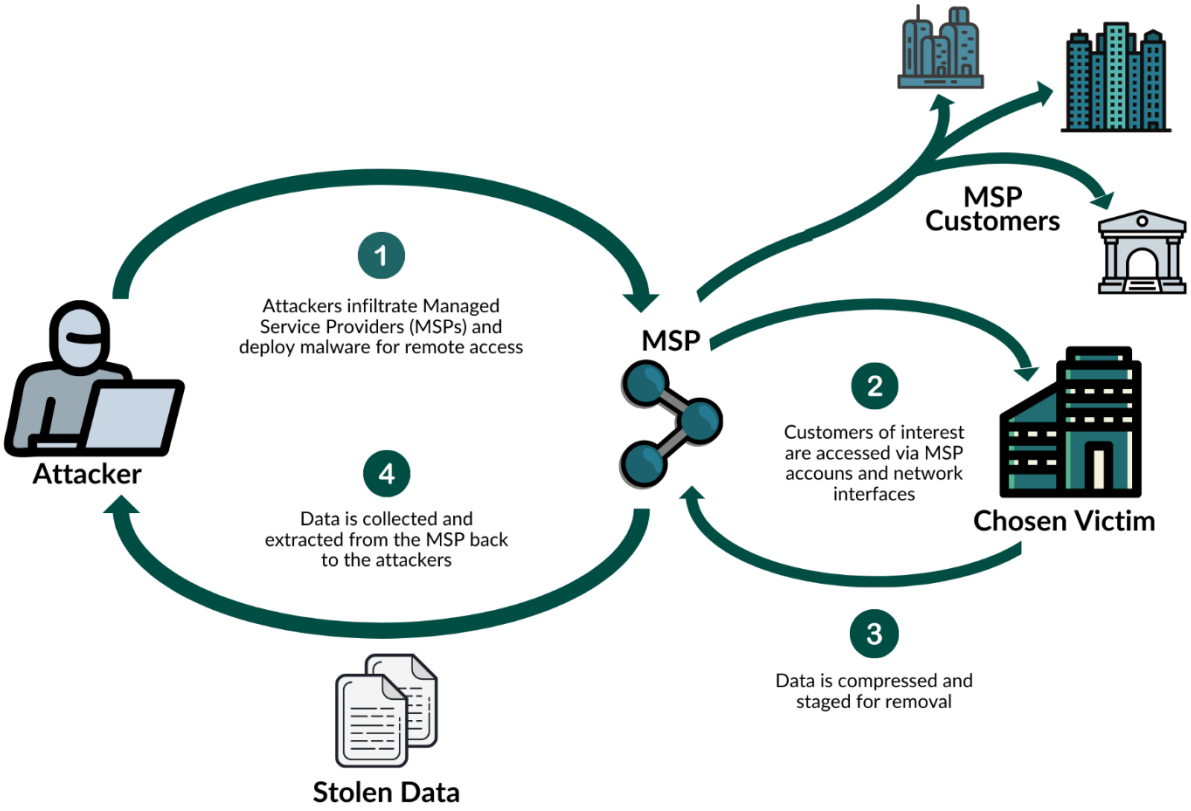

Figure 1 – Operation Cloud Hopper[6]

Again, this was highlighted in the EU-wide risk assessment:

> *"**Lack of access controls:** a subcontractor with administrator's privileges on the network performs adverse action, leading to confidentiality/integrity and/or availability breach. The subcontractor's action may be due to a legal requirement imposed by a third country or rogue behaviour of the contractor's staff."*

In order to manage the risk associated with administrative third party access it is imperative that operators insist on strict access control procedures for third parties and closely monitor and supervise their activity on the network.

Ultimately whilst operators may choose to outsource responsibility for the operation of certain aspects of their network to third parties they cannot outsource accountability and thus must ensure they have adequate processes in place to supervise third parties.

[6] https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html

7 Security Measures

The operator should implement the Supply Chain Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
SC.01	The operator shall assess the risk profile of their critical suppliers against a range of technical and non-technical criteria as part of their procurement processes and ongoing supplier management.
SC.02	The operator shall have a detailed understanding of its supply chain, including subcontractors of critical suppliers. The operator should request its critical suppliers to outline their supply chain contingency plans to ensure continuity of service.
SC.03	The operator shall include security as part of its product or service testing and evaluation process. The operator's senior security personnel shall be involved in the entire product or service acquisition lifecycle.
SC.04	Security requirements shall be developed, agreed and documented as part of contractual arrangements between operators and their critical suppliers. The operator should ensure these requirements are passed down through the supply chain.
SC.05	Contractual arrangements with suppliers shall highlight security as a shared responsibility between the operator and suppliers.
SC.06	Suppliers shall be contractually required to provide timely notification to the operator of security incidents or vulnerabilities in their network equipment.
SC.07	Suppliers shall be contractually required to support the operator in investigating and remedying security incidents on their networks.
SC.08	The operator shall control and monitor third party access to its networks, ensuring third party access does not reduce the overall security of the network in line with ECSM 005.
SC.09	The operator shall require third parties to have security measures equivalent

	the operator's own security measures in place when accessing the operator's network.
SC.10	Third parties shall be granted the minimum access required to perform their functions on the operator's network, and this access shall be reviewed periodically.
SC.11	The operator shall retain sufficient expertise to adequately monitor and supervise third parties accessing their network.
SC.12	The operator should avoid building up a long-term dependence on an individual supplier and shall put in place contingency plans which minimise disruption should switching supplier be required.
SC.13	The operator should require suppliers to achieve suitable European cyber security certifications for critical products and services, where such schemes exist.[7]

139
140
141
142

[7] The EU Cybersecurity Act ((Regulation (EU) 2019/881) establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes. 5G Certification has been highlighted as a priority area for cybersecurity certification .

8 Implementation Guidance

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in Table 1**Error! Reference source not found.** below.

Table 1 - Correlation of implementation Guidance to Security Measures

	SC. 01	SC. 02	SC. 03	SC. 04	SC. 05	SC. 06	SC. 07	SC. 08	SC. 09	SC. 10	SC. 11	SC. 12	SC. 13
8.1	✓	✓	✓									✓	
8.2					✓	✓	✓		✓	✓			✓
8.3				✓				✓		✓			
8.4				✓				✓	✓	✓	✓		
8.5	✓	✓	✓	✓					✓		✓		✓

8.1 Assessing the Risk Profile of Suppliers

Applicable Security Measures: SC.01, SC.02, SC.03, SC.12

Network operators should assess any critical suppliers against a range of technical and non-technical criteria as part of their procurement processes and ongoing supplier management. These assessments should determine whether a supplier is used in critical parts of the operator's networks, as well as the ongoing level of security oversight and supervision the supplier is subject to.

8.1.1 Technical Assessment

Technical assessments should consider at least the following criteria -

- Product quality & performance,
- Product development lifecycle management,
- Product security management,
- Vulnerability management,
- Update & Patching,

- Secure configuration,
- Details of third party software and code,
- Equipment interoperability,
- Recognised assurance or certification schemes that the supplier has achieved.

Technical assessments should be based on independent verifiable evidence and not information provided by the suppliers themselves, wherever feasible. Where it is required to receive evidence from suppliers, operators should verify this through their own or independent third-party testing. Recognised assurance and certification schemes, particularly such as European certifications, are encouraged in this regard.

8.1.2 Non-technical Assessment

Non-technical assessments should consider at least the following criteria -

- The supplier's business practices,
- The relationship between the supplier and a non-EU States,
- The legal and regulatory framework in the supplier's country of main establishment,
- The ability of the supplier to assure continuity of supply,
- The supplier's previous record of security and transparency.

It is acknowledged that operators may not always have the information available to assess some of the non-technical criteria, however, where this information is available either through open sources, or provided by State authorities, it should form part of an operators overall risk assessment of critical suppliers in evaluating all options and alternatives.

8.2 Contractual Arrangements

Applicable Security Measures: SC.05, SC.06, SC.07, SC.09, SC.10, SC.13

Strong contractual arrangements help operators to ensure that they can enforce and pass down appropriate security requirements through their supply chain which should be contractually enforceable. It is imperative that the operator's senior security staff are involved in setting the minimum security requirements to which a supplier is subject.

To ensure that the supplier applies at least the same standards of security as the operator, the operator should ensure the supplier is required to observe the same policies, procedures and training packages that apply to the operator, to the extent that such policies may impact on the security of the network.

Operators should consider at least the following security requirements in contractual arrangements with critical suppliers:

- Level of access required for supplier and classification of data being accessed.
- Legal and regulatory requirements such as data protection, privacy, intellectual property and copyright to which the supplier is subject.
- Agreed controls for both suppliers and operators concerning physical and environmental security, access control, network design, logging, monitoring and auditing.
- Explicit list of authorised personnel to access operator's network or agreed process for operator authorisations for supplier personnel to access network.
- Operator's policies to which the supplier will be subject to.
- Any training or awareness programs required for supplier personnel.
- Incident management procedures, including incident notification requirements and supplier obligations in responding to incidents. The supplier should notify the operator of significant incidents and product vulnerabilities within a minimum of 72 hours of becoming aware of the incident.
- Vulnerability management including agreed schedules for critical vulnerability patching.
- Requirements for sub-contractors and the requirement to pass down security measures to their suppliers.
- Right to audit suppliers and/or any certification requirements.
- Break clauses, penalties and remedies for any failure to meet contractual requirements.

Operators should have an ability to continuously monitor their supplier's adherence to agreed contractual obligations.

8.3 Data Transfers to the Supply Chain

Applicable Security Measures: SC.04, SC.08, SC.10

Operators should share the minimum amount of data necessary with suppliers, consistent with Irish and EU data and privacy protection rules. Whenever feasible the operators should host any data they wish to share with suppliers on their own systems, and prevent this data

being removed to third party supplier systems. Where technically feasible, efforts should be made to obfuscate any personal data. If data must be transferred off the operator's network and into the supply chain, there should be a process to authorise the transfer, validate that the data has arrived, and a requirement that the supplier declares that the data has been deleted irretrievably when the reason for the transfer is completed.

The operator should be aware of and authorise all entities accessing their data, as well as being aware of where the data will be accessed from, and make appropriate, risk-based decisions whether to allow the access or not. The operator should confirm by both audit and testing that the security of their data, wherever it is held in the supply chain, is at least as secure as it would be in the operator's own systems and is in all cases consistent with Irish and EU data and privacy protection rules as stated.

8.4 Third Party Administrative Access to Networks

Applicable Security Measures: SC.04, SC.08, SC.09, SC.10, SC.11

Operators may require third parties to have privileged access to their networks to carry out routine maintenance or to resolve issues as part of vendor third line support, or they may have engaged an MSP to operate certain network functions. As outlined in the overview of risk section these third party administrators present attractive targets to attackers, and therefore a higher level of security is required.

The level of security and associated controls applied to third parties should be at least as rigorous as the level applied to the operators own employees. Contractual arrangement will be critical in enforcing these requirements. ECSM 005 – Network Management and Access Control highlights the baseline security measures for network access.

Specifically, the following should apply to third parties who are granted administrative access to the operator's network:

- The operator controls the accounts and authorisation for third party administrative access. The accounts are authenticated to individuals, and the operator maintains a record of these accounts.
- Multi-factor authentication (MFA) is required for administrative access to the network.
- The operator should not allow routine or direct access to its network by third parties, and should instead be through an appropriate mediation point such as a jump server, which the operator controls.

- The operator and the third party should log and monitor all access to the operator's network.
- In the case of equipment vendors who are required to access the network for routine or ad hoc maintenance or updates their access should not be persistent. Instead the access should be granted by the operator, ticketed, time limited and use a one-time password.

8.5 Audit and Assurance

Applicable Security Measures: SC.01, SC.02, SC.03, SC.04, SC.09, SC.11, SC.13

Whilst outsourcing or resource-pooling is a legitimate business practice, accountability for the security of the network remains with the operator. Therefore, whilst it would not be expected that the operator retains the same level of technical expertise as their third party contractors/suppliers, they must at least retain the ability to assess the performance of their suppliers, as well as an ability to monitor and supervise their activities in order to assure the overall security of the network.

This means the right to audit should be included in contractual arrangements with suppliers. Audits should be carried out either by the operator themselves, or an independent third party. Any audit or review should be carried out by technically competent people who understand electronic communications networks or IT systems. The operator's security team should be involved in the establishment of the test requirements as well as reviewing the results. The purpose of the audits and testing is to enable to operator to ensure that the data accessed or held by the supplier is as secure as it would be if it were held on the operators own network. The audit should examine the appropriateness or otherwise of the contractual agreements between the operator and the supplier. Operators should know their obligations regarding privacy and data protection under EU and Irish law and reflect these obligations in their contracts.

Regular audit and certification can be used by a supplier to demonstrate to multiple clients that they are meeting the security requirements set out as part of contractual arrangements. This arrangement can somewhat negate the need for the operator themselves to conduct audits, however, they should have access to the certification reports and be assured that the certifications meet the security requirements agreed as part of contractual arrangements.

Operators should avoid developing a long-term dependence on any individual supplier and should retain the ability to change suppliers should the need arise. Retaining a level of in-

house expertise for critical network functions, in the event of a failure of a critical supplier, should be considered.

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 ISO-IEC 27001/2: Information technology — Security techniques — Information security management systems

ISO - ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems

Clause 15 – Supplier Relationships contains detailed controls and implementation guidance on how to ensure the protection of an organisation's assets that are accessed by suppliers. It covers how information security requirements can be agreed, documented and enforced with suppliers. It also provides information on securing the organisations supply chain, including how to monitor supplier's compliance with security requirements.

This standard is copyrighted and available to purchase through national standards agencies.

9.2 ISO/IEC 27036 – Information technology — Security techniques — Information security for supplier relationships

ISO - ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems

ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships, rather than retailing, and information-related products.

It covers the entire supplier relationship lifecycle:

- **Initiation** - scoping, business case/cost-benefit analysis, comparison of insource versus outsource options as well as variant or hybrid approaches such as co-sourcing;
- **Definition of requirements** including the information security requirements;
- **Procurement** including selecting, evaluating and contracting with supplier/s;

- **Transition** to or implementation of the supply arrangements, with enhanced risks around the implementation period;
- **Operation** including aspects such as routine relationship management, compliance, incident and change management, monitoring etc.;
- **Refresh** - an optional stage to renew the contract, perhaps reviewing the terms and conditions, performance, issues, working processes etc.;
- **Termination and exit** - ending a business relationship that has run its course in a controlled manner, perhaps leading back to step 1.

9.3 NIST Cyber Security Framework

Cybersecurity Framework | NIST

Supply Chain Risk Management (ID.SC) outlines 5 high level outcomes an organisation should achieve in order to protect their supply chain and supervise third party compliance:

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

- **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
- **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber Supply chain risk assessment process.
- **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers .

9.4 NIST SP 800-53

SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

The family of controls titled **SA – System and Services Acquisition** provides an in-depth overview of controls that an organisation can put in place throughout the entire lifecycle of an information system, from acquisition through its operation until retirement. It also contains controls and guidance on topics, such as, inter alia, trustworthiness, supply chain protection, security testing and evaluation

9.5 NIST SP 800-161: Supply Chain Risk Management Practices

SP 800-161, Supply Chain Risk Management Practices for Fed Info Sys and Orgs | CSRC (nist.gov)

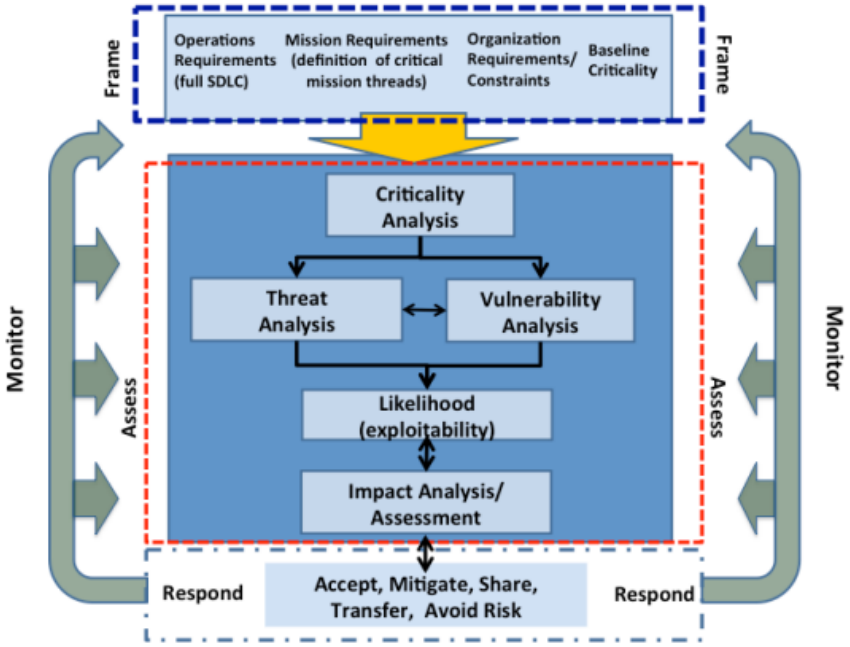

Figure 2: NIST Supply Chain Risk Management Process

Supply Chain Risk Management Practices provides guidance to organisations on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations; how to integrate ICT Supply Chain Risk Management (SCRM) into overall risk management activities by applying a multi-tiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities; and builds on existing practices from multiple disciplines and is intended to increase the ability of organizations to

strategically manage ICT supply chain risks over the entire life cycle of systems, products, and services.

9.6 ENISA Security Supervision under the EECC

Security Supervision under the EECC — ENISA (europa.eu)

5G Supplement - to the Guideline on Security Measures under the EECC — ENISA (europa.eu)

This document provides advice specifically tailored to providers of Electronic Communications Networks and Services and competent authorities which supervise them. Security Objective 4 - Security of Third Party Assets has three levels of measures that operators can implement basic, industry standard and state-of-the-art. The complementary 5G security supplement offers further detail and controls that are applicable, in line with the measures outlined in the EU 5G Security Toolbox.

9.7 ENISA Supply Chain Integrity

Supply Chain Integrity: An overview of the ICT supply chain risks and challenges — ENISA (europa.eu)

This report identifies supply chain threats and examines the strategies that may be used to counter them. The report recommends that participants in the supply chain follow a core set of good practices that can provide a common basis to assess and manage ICT supply chain risk – and to recognize that governments must work in collaboration with private industry to build international assessment frameworks. Such frameworks should be: risk-based and grounded in good threat modelling, transparent, consistent, flexible standards-based and based on recognition of the reciprocity that characterizes international trade relations.