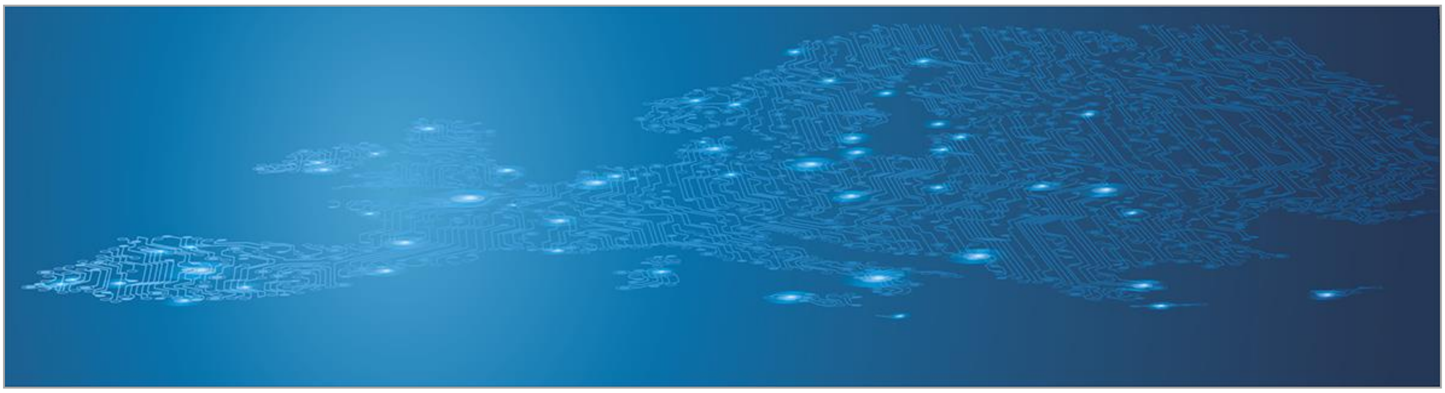

Secure ICT Procurement in Electronic Communications

Analysis and recommendations for procuring ICT securely in the Electronic Communications Sector

December 2014

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Christoffer Karsberg, Dr Marnix Dekker

Contact

For contacting the authors please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This work has been carried out in collaboration with EY Luxembourg, in particular: Céline Frédéric, George Tountas, Alexandre Minarelli and Brice Lecoustey.

We have received valuable input and feedback from a range of experts from Electronic Communication providers and vendors. In particular we would like to thank the contributions from NOS (Pedro Gomes Silva, Pedro Gaspar Moreira), Huawei (Wouter van Wijk, David Francis), Telefonica (Domingo Javier Hernandez, Juan Carlos Gomez Castillo, Manuel Carpio Camara, Patricia Diez Muñoz), Netnod (Kurt Erik Lindqvist) and Telecom Italia (Antonietta Alfano, Gensèric Cantournet).

Also we would like to thank the experts from the ENISA Electronic Communication Reference Group for providing us useful feedback during meetings, interviews and reviews of drafts of this document.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-116-8, DOI: 10.2824/094009

Executive summary

Society is dependent on secure electronic communications services (mobile and fixed telephony and Internet access etc.), which at the same time become more and more complex in terms of technology and actors involved. Hardware and software play a critical role in the core operations of electronic communications networks and services and are most of the time procured by specialized ICT suppliers and outsourcing partners. This leads to providers being increasingly reliant on third parties to ensure the security and resilience of their own infrastructure and this also exposes them to additional security risks.

According to the latest ENISA Annual Incident Reports 2013[1], most incidents reported between 2011 and 2013 were caused by failing hardware or software. In discussions with electronic communications service providers, they have indicated that there are sometimes problems or misunderstandings in vendor-provider relationships and outsourcing in general.

The goal of this report is to analyse the importance of managing the security risks involved in the procurement and outsourcing process. More specifically, it emphasises on the risks which could lead to a disruption of electronic communications services for users.

ENISA has performed a survey with providers and vendors to collect issues and practices and a desktop research of existing initiatives.

The surveyed providers mainly have the following concerns when procuring key ICT products and outsourcing services for core operations:

- Lack of adequacy and effectiveness of the security controls on the vendor's side;
- Potential vulnerabilities the provider can be exposed to due to (unknown) flaws in ICT products or services;
- Non-compliance with security requirements defined in the contract on the vendor's side
- Lack of adequate support from vendor in case of breakdown;
- Weak negotiation power for the provider to enforce specific security requirements;
- Lack of framework or guidelines from the industry to guide providers during the procurement and outsourcing process.

The survey has indicated that many providers have a policy or framework in place to manage the security issues experienced during the procurement or outsourcing of ICT products and services. The security framework usually focuses on the following areas:

- Assessing the risks providers may face when buying ICT products or outsourcing ICT services.
- Articulating clear, actionable and measurable security requirements which will help the providers to prevent or mitigate the risks identified during the risk assessment.
- Continuously monitoring the performance of its vendors based on the contract, in order to assess its compliance with security requirements.
- Agreeing with the vendor on a change management process in order to define how to handle potential changes in security requirements or the complete termination of the contract.

ENISA acknowledges however that providers adopt different approaches when dealing with security risks involved in the procurement or outsourcing process. For these reasons and to meet expressed concerns, this report presents an overview of practises used in the sector and gives the following general recommendations:

[1] ENISA (2014), Annual incidents report 2013, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013

1. Member States should promote the awareness about security risks related to ICT procurement and outsourcing
2. Vendors, providers and critical customers should develop a collaborative approach to defining security requirements, to sharing information about security vulnerabilities and threats, and to the mitigation of incidents

Recommendations to providers of electronic communications networks and services are as follows:

3. Engage internal stakeholders and develop a holistic risks management approach
4. Conduct a risk assessment before procuring or outsourcing to third party
5. Develop high level security policy and requirements before selecting preferred vendor
6. Develop clear, solid, measurable and actionable security requirements for vendors
7. Prioritize the implementation of the security requirements for vendors
8. Manage security risks through the procurement lifecycle
9. Monitor the performance of your vendors

1 Introduction

The world today is depending more and more on electronic communication. Society is becoming heavily reliant on communication services and people expect to be connected anywhere and at any time. As a consequence, customers are more and more demanding reliable and secure services, and they depend on their providers of electronic communications networks and services.

The importance of resilience in an electronic communications service provider's network is visible when significant security incidents hit customers, and when creating issues with important functions of society. In the last years, network outages have been reported in many parts of the EU, affecting both mobile and fixed communication providers. According to the ENISA Annual Incident Report 2013[2], most incidents reported were caused by technical/system failures (i.e. 61% of the incidents in 2013 – Figure 1) and more specifically hardware failures and software bugs. Network assets most affected by system failures were switches and Home Location Registers (HLR). These network components, which are essential parts of core operations of networks, are naturally vulnerable to failures.

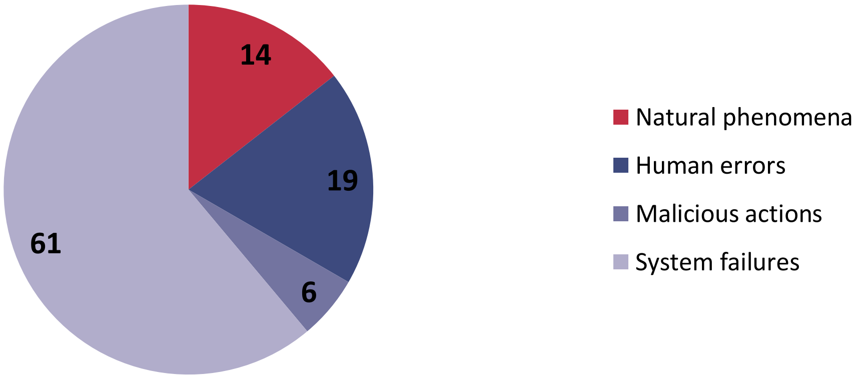

Figure 1: Incidents per root causes (2013)

An example of a system failure involving a HLR, was an incident with a mobile operator that in 2012 experienced an important network outage leaving mobile customers without electronic communications services for 21 hours. The outage was caused by a failure in the HLR while the mobile operator was extending its outsourcing relationship regarding the field maintenance and switch sites to include the complete operation of the network[3]. The detailed customer information disappeared during the transition process leaving handsets unable to authenticate their users. Without the database and all customers' information, mobiles and other devices were gradually forced off the network. The same kind of scenario can similarly impact other providers.

Due to the complexity of electronic communications networks components and services, providers are to different extents using suppliers to provide them with specific ICT products and services. Naturally, most of the providers buy their infrastructure components from ICT vendors while a large range of them also outsource a part of the network operations to an outsourcing partner. This means that they become reliant on third parties to ensure the security and resilience of their own infrastructure, but also that they can be subject to additional security threats.

[2] ENISA (2014), Annual incidents report 2013
[3] The Register, http://www.theregister.co.uk/2012/07/13/o2_outage_cause/

In discussions with providers, they indicated that there are sometimes problems or misunderstandings in the vendor-provider relationships and outsourcing in general. More specifically, providers are not always empowered to effectively manage the security risks involved in these relationships. For this reason, in discussions with providers, ENISA has been asked to study this topic and to develop guidelines with security requirements aimed at vendors. These requirements could be applied in the procurement or outsourcing phase to support the providers in managing security threats and guaranteeing the resilience of their networks after the introduction of third party products and services.

Policy context

The reform of the EU legal framework for electronic communication, which was adopted in 2009 and came into effect in May 2011, adds Article 13a to the Framework directive. Article 13a addresses the security and integrity of public electronic communications networks and services. The legislation concerns National Regulatory Authorities (NRAs) and providers of public electronic communications networks and services (providers).

Among other things, article 13a states the following:

- Paragraph 1 requires the provider to take measures to "prevent and minimise the impact of security incidents on users and interconnected networks".
- Paragraph 2 requires the provider to "take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services".
- Paragraph 3 requires the provider to "notify the competent National Regulatory Authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services".

Providers are liable towards the users of their services and the respective NRA for the security of their electronic communications services, through the transposition of the above mentioned Article in member States' legislation. Liability cannot be transferred to a third party, although providers may be dependent on suppliers of third party products or services used for their core operations. For that reason it is important that the security measures the providers are liable for are extended to their vendors through their contractual relationships.

More information about ENISA's work on Article 13a, and the Article 13a Expert Group of NRAs, can be found at: http://resilience.enisa.europa.eu/article-13.

Goal and Scope

The goal of this report is to analyse the importance of managing the security risks involved in the procurement and outsourcing process of key ICT products and services. More specifically, it emphasises the risks which could lead to a disruption of services for the customers.

Together with this report a separate Security Guide[4] has been produced to support primarily electronic communications service providers, but also ICT vendors, with practical guidelines to better manage potential security risks in products or services, which could lead to disruptions in electronic communications services.

[4] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors

Target audience

This report is aimed at the actors in the electronic communication sector (Providers, Vendors, NRAs, Information Security Professionals, etc.).

The report informs the actors about issues and concerns of the sector regarding potential security threats when buying or outsourcing ICT products and services from third parties, current initiatives and processes used by providers to manage the same and, based on issues and findings, gives general recommendations to the actors in the sector.

Methodology

In order to gather experience and opinions from experts in the field, an anonymous online survey across European electronic communications service providers was launched. 29 providers responded to this survey, bringing insights about their main concerns and areas of focus when buying ICT equipment or outsourcing ICT services, the type of security policy they have in place and the main security requirements they apply to their suppliers to prevent or mitigate security risks. The mix of providers participating in this survey represents a wide coverage in terms of security practises applied based on the type of electronic communication services provided (figure 2). Note that most of the participating providers are offering multiple services to their customers.

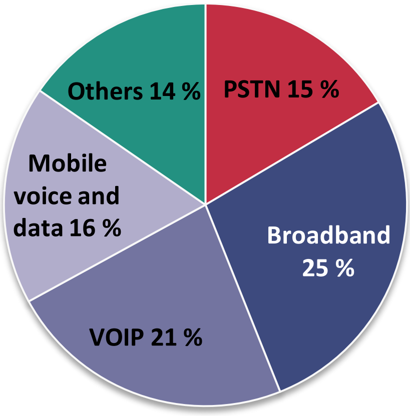

Figure 2: Types of services provided by survey's respondents

In addition to the online survey, there have been interviews with experts from the electronic communications industry, 10 electronic communication service providers and 2 vendors, asking them qualitative questions about their views and experience with security risks involved in the procurement and outsourcing process of key ICT products and services. Guidelines were gathered from them on best practises in terms of security requirements and controls which should be applied to vendors to prevent or mitigate such security risks.

Consequently a desktop study followed. Initiatives already taken by the industry were analysed, regulatory frameworks or guidelines issued by National Regulatory Authorities (NRA) were looked into and a range of standards and good practises were reviewed as suggested by the industry, such as relevant ISO standards and the SAFECode leading practises.

Structure of this document

This document is structured as follows:

- In section 2 the dependencies of electronic communications service providers on third parties for the provision of key ICT products and services are described. ICT product supply chains and outsourcing services are successively approached.
- Section 3 describes concerns raised by providers during the survey. It focuses on issues surrounding the management of the security risks and the implementation of security requirements in the context of third party products and services. The issues are attributed a number (Issue #1 etc.) and are referred to in the following three sections.
- In section 4 national regulatory frameworks and guidelines are described, followed by a description of industry standards and leading practises.
- In section 5 the report presents a security framework with main measures used by electronic communications service providers to ensure a constant level of resilience after the introduction of third party products and services into their infrastructure, together with high level security requirements commonly applied to vendors.
- Lastly, in section 6 the report concludes with recommendations to the actors of the electronic communications sector, with the aim to support them in the security management involved in the procurement and outsourcing processes.

2 About Procured Products and Outsourced Services for Core Operations

It is probably not an exaggeration to say that all electronic communications service providers depend to some degree on their suppliers. Indeed, most of the providers around the world, whatever their size, their market position or their core services, have relationships with suppliers that provide them with ICT products or managed services. Most of these products or services play a critical role within the providers' networks, and a disruption in those could have an immediate impact on the services offered to their customers. There is a need for the electronic communication service providers to carefully manage security risks involved in their procurement and outsourcing relationships to ensure a constant level of resilience despite the introduction of third party products and services into their infrastructure. This means that the providers should work closely with vendors to adopt good practises in terms of security risk management.

2.1 ICT products supply chain

In general, it is common practice that suppliers provide electronic communications service providers with ICT products and equipment, which will then be integrated into their network infrastructure. Most of the components in a network are acquired from specialized and large ICT vendors. This includes both software and hardware components, which are part of a complex environment. Below we take a mobile network infrastructure as an example.

As shown in figure 3, several components shape a mobile network infrastructure and mobile operators generally buy these components, from the access network components (Antennas, Base Transceiver Station, etc.) to the core network components (HLR, GGSN, Intelligent Network). This example is illustrative but other electronic communication networks present similar complexity.

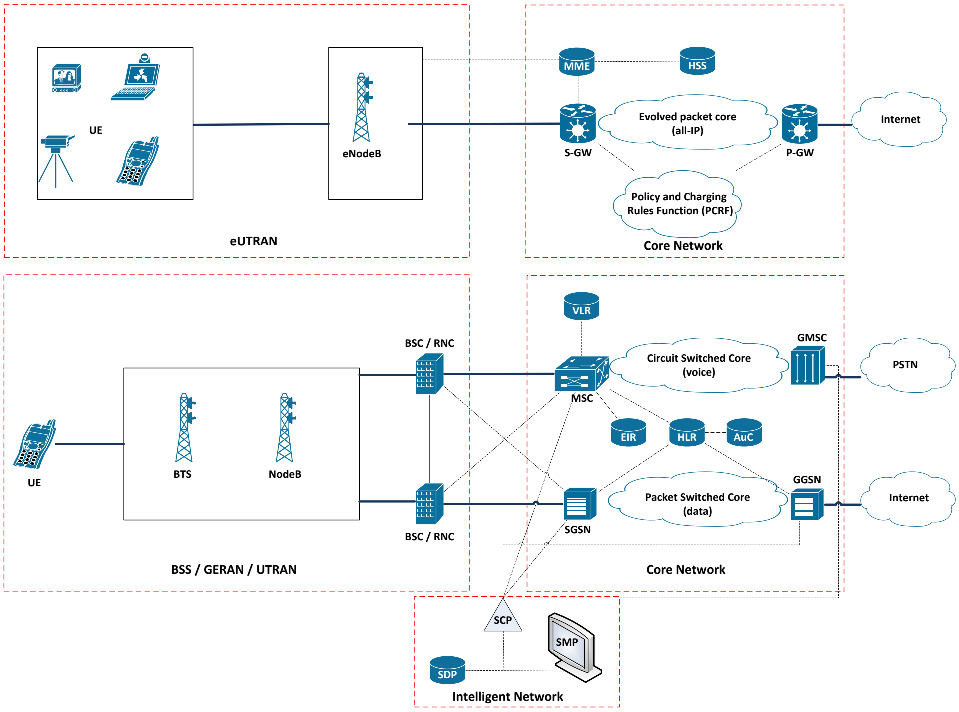

Figure 3: Complex network environment (Mobile 2G, 3G, LTE) - illustrative[5]

[5] Theoretical, source EY Luxembourg

Nowadays, the ICT products supply chain is becoming more and more globalized and complex, bringing additional challenges and dependencies for a provider. Multiple components designed, developed and manufactured in different countries are now combined to produce a single hardware or software later acquired by an electronic communication service provider through a single vendor.

Each member of the global ICT product supply chain has the responsibility to ensure the security and the resilience of the final product. Taking that into consideration, a provider is becoming dependent on the supplier's downstream suppliers in case of security issues with one single product. This creates the risk of lack of visibility, understanding, traceability and control over the ICT products for the providers and increases the risk of counterfeit, malicious or untrustworthy products. As a result, there is a need for the provider to use specific security frameworks to better manage evolving security risks involved in the acquisition of ICT products from suppliers.

2.2 Outsourced services

Suppliers can also provide electronic communications service providers with services "in support of a business function for performing activities using suppliers' resources rather than the ones of the acquirer"[6] (i.e. human resources, infrastructure, etc.) to perform a specific operation. This involves a long-term outsourcing contract covering a business operation (e.g. billing, HR, etc.), a network operation (e.g. maintenance, strategy development, construction, integration, and even full scale operation of networks and services etc.) or a top layer application (e.g. value added services). Typically, the vendor acts under a service level agreement with full responsibility for the activities specified in the outsourcing contract.

Unlike the outsourcing of business operations such as billing or HR function, the outsourcing of network operations can impact the availability of the provider's core service. As shown in figure 4, an organization can outsource its complete network operation or a part of it, such as network planning, network design and engineering ("PLAN"), network installation and integration ("BUILD"), or network operations and maintenance ("RUN"). Among this last function, a provider can split its outsourced services by network operations or field services.

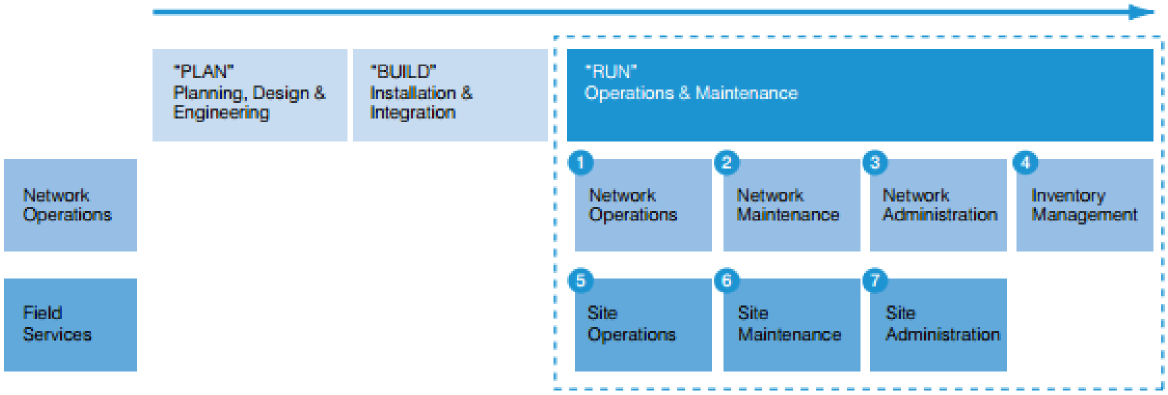

Figure 4: Network operations which can be outsourced[7]

Electronic communications service providers are planning to spend about $79 billion in 2017 on outsourced network tasks to equipment vendors, which represents 8 % of annual growth rate[8] from 2012 to 2017[9].

[6] ISO/IEC International Standard 27002 (2005), Information technology — Security techniques — code of practice for information security
[7] Bookz & Company Inc (2009), Outsourcing network operations: Maximizing the potential
[8] Compound Annual Growth Rate : the year-over-year growth rate of an investment over a specified period of time
[9] Infonetics (2013), "Telecom equipment vendors manage 45% of the world's subscribers as outsourcing grows"

While outsourcing is bringing several benefits to a company, it is also bringing security challenges such as difficulties to align internal security objectives with suppliers' policies, lack of security controls, failures to accurately monitor the security performance of the supplier, etc. As a result, there is a need to implement an information security governance framework toward outsourcing suppliers. Indeed, savings from outsourcing could be offset by security incidents, so security threats need to be taken into account from the first stage of the outsourcing process, to ensure that the benefits of outsourcing can be realized despite security costs and constraints. On the other hand, suppliers of outsourcing services should be able to properly manage the risks involved in the outsourcing process, meet clients' requirements while still making a commercial profit. This means that electronic communications service providers should be ready to accept an increase in price when imposing strong security requirements.

3 Issues and Concerns expressed by providers

In the online survey and interviews with providers and vendors, a set of issues were collected that the surveyed providers are concerned with when buying or outsourcing key ICT products and services. The main concerns that were expressed include (but are not limited to):

- **Lack of adequacy and effectiveness of the security controls on the vendor's side (Issue #1)**

Providers are worried that the security measures that the vendors are applying by default will not be adequate to protect their infrastructure. They are afraid that vendors' security controls would not be aligned with their own security objectives and would fail to prevent the security risks they have identified. The providers want to receive the assurance from their vendors that relevant controls are in place and operate correctly to meet the minimum acceptable level of residual risk they have defined.

- **Potential vulnerabilities providers can be exposed to due to (unknown) flaws in ICT products or services (Issue #2)**

The interviewees are concerned about vulnerabilities, and especially potential blind spots, unknown vulnerabilities, in products or services. This is also highlighted by the United States Government Accountability Office (GAO) (2013), see section 4.1.1, which states that the main concerns of electronic communication service providers when buying or outsourcing are the anomalies that could arise from procured products because of low quality, lack of controls or potential errors (i.e. erroneous coding in the software). The providers want to be made aware of any vulnerability affecting the product or service they buy and any potential issues they can face with their equipment.

In addition, the providers wish to be informed by the vendor as soon as possible if another provider has had issues with the same products they have procured, in order to fix the problems before it actually affects their customers.

- **Non-compliance with security requirements defined in the contract on the vendor's side (Issue #3)**

Another concern expressed in our interviews was that sometimes providers experienced vendors deviating from agreed contracts or "taking shortcuts" in order to cut down costs or time to deliver and as a result fail to comply with security requirements defined in the contracts leading to increased security threats.

- **Lack of adequate support from vendor in case of breakdown (Issue #4)**

Electronic communication providers expressed their worries regarding potential lack of support from their vendors and outsourcing partners in case of incidents. More specifically they were concerned with the level of responsibility the vendors are willing to accept as well as their response time. They wanted to be assured that they would be supported by trained and skilled people in case of major incidents and especially in order for their core services to recover quickly.

- **Weak negotiation power for provider to enforce specific security requirements (Issue #5)**

Providers were concerned about the inherent lack of negotiation power they have, since options on the market are limited. Some providers expressed that in some cases there could be a non-proportional increase in costs and time to market in vendor offers when requesting additional security measures.

- **Lack of framework or guidelines from the industry to guide providers during the procurement and outsourcing process (Issue #6*)***

Providers raised their concern about a lack of unified guidelines to help them dealing with security risks involved in the procurement and outsourcing process. Despite the existence of standards related to electronic communication security, providers have highlighted the lack of an integrated and unified approach which will support them in specifically dealing with security risks involved in the procurement and outsourcing process.

Through the review of existing initiatives, we observed that only a few national regulatory authorities consider specifically the management of security risks involved in the relationships providers have with ICT vendors into their national guidelines (i.e. UK, Australia, USA and India). In addition, our online survey showed that 72% of the respondents stated that there is no regulatory framework to govern their requirements regarding third party products and services.

Besides, the online survey showed that not all of the providers themselves apply security requirements to their ICT vendors. About 7 % do not consider security requirements for ICT vendors, see figure 5 below, while most of them have different approaches for preventing or mitigating potential security threats when buying from or outsourcing to third party. Through the online survey, we observed a significant divergence between answers regarding content and levels of security requirements. Even if all providers in our survey define Service Level Agreements with their vendors, the importance of security requirements depends highly on the provider's internal practises. As shown in figure 5, some providers tend also to adapt the security requirements based on the type of products/services supplied and/or based on the criticality of the products/services supplied. It could also be the case that security requirements are adjusted based on the existing relationships providers have with the vendors (e.g. in case of long and trustful relationship with the same supplier).

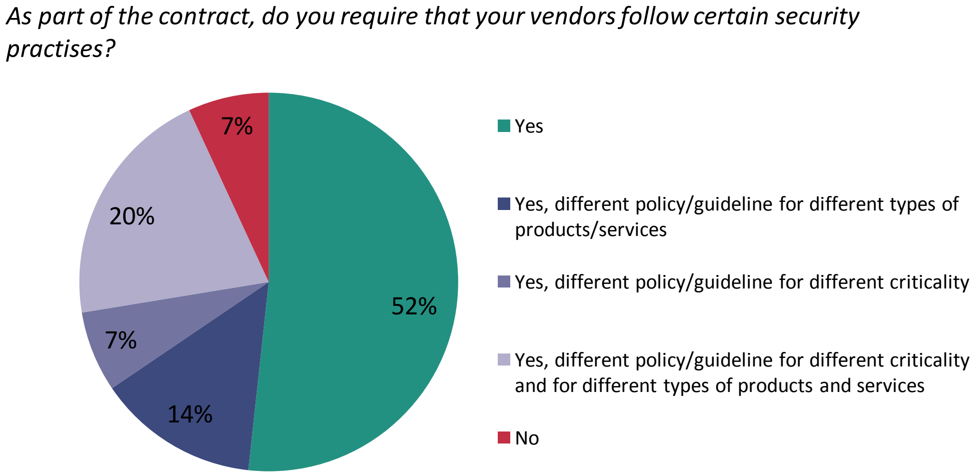

Figure 5: Divergence in approach in developing security requirements

4 Existing initiatives supporting providers

4.1.1 National regulatory frameworks

We have reviewed some existing regulatory frameworks and guidelines to identify existing approaches which could be taken as examples for the management of security risks involved in the procurement and outsourcing of key ICT products and services to third parties. Even if the goal of this report is not to advise on an approach or another, it provides some comparable points of view.

We provide examples from four countries around the world which advocate through regulatory frameworks the resilience of the electronic communications sector targeted on risks involved in relationships with third parties.

A. United Kingdom[10,11,12]

In May 2011, EU Member States were required to implement Article 13a and 13b in national law as requested by the EU Telecom Framework Directive. The UK's Office of Communication (Ofcom) complied with this requirement by revising the Communication Act 2003 (CA2003), principally by adding the Sections 105A-D.

The guidance focuses on two main areas:

- *Risk management*: electronic communication service providers and vendors must take care of their networks, applying appropriate measures to manage security risks including *management of general security risks*; *protecting end users*; *protecting interconnections*; and *maintaining network availabilit*y.
- *Incident reporting*: Vendors and electronic communication service providers must report to Ofcom any security breaches or reductions in availability which have a significant impact on the network or service. This significant impact is measured through thresholds given for different types of networks and outages.

To ensure the above, Ofcom expects providers to develop and implement appropriate risk management or mitigation actions. In case of doubt about the compliance to the requirements, Ofcom can request providers to perform an audit of their systems and impose financial penalties.

Due to the increased importance of outsourcing in the electronic communication service industry, Ofcom have started considering that security requirements should be applied during the outsourcing or procurement process (section 105 A – Management of general security risks).

According to Ofcom, providers should take the appropriate measures to mitigate security risks coming from their supply chain. Ofcom expects providers to perform a risk assessment and implement mitigations actions before entering into a new outsourcing relationship or implementing new equipment into their network. In addition, the providers should have sufficient technical and management expertise among its staff to manage potential security risks.

[10] Ofcom (2012), Ofcom guidance on security requirements in the revised Communication Act 2003: Implementing the revised EU Framework.
[11] Ofcom (2014), Updating Ofcom's guidance on network security.
[12] Ofcom (2014), Ofcom guidance on security requirements in sections 105A to D of the Communication Act 2003 http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/

B. United States

The United States Government Accountability Office (GAO) was requested to conduct a study in 2013 on actions taken by federal institutions and electronic communication service provider to deal with security risks involved in the procurement or outsourcing of foreign ICT products and services.[13]

It has been highlighted that the main concerns of the providers are not related to the provenance of the products and services but rather the anomalies that could arise from procured products because of low quality, lack of controls or potential errors (i.e. erroneous coding in the software) (**Issue #2**)

In order to deal with these problems, GAO study highlights three ways that companies have started following in order to mitigate this problem:

- Some companies have developed their own practices based on national and international standards regarding information systems' security (ISO, IEC, NIST, Internet Engineering Task Force…).
- Other companies have participated in cybersecurity groups such as The Open Group Trusted Technology Forum (OTTF) and The Communication Sector Coordinating Council (CSCC). This last group has the objective to facilitate the coordination between industry and the federal government to improve physical and cyber security of the infrastructure through the creation and adoption of standards.
- Lastly, providers have adopted voluntary security management procedures which cover the entire life cycle of their equipment:
  - **Vendor Selection:** When the providers select their vendors, they usually focus on the vendor's security practices, their use of security-related standards and their reputation to manage security issues. Their practices depend highly on the criticality of equipment or services being procured.
  - **Vendor Security Requirements:** Some companies force vendors to comply with requirements covering the physical security of products, the access restriction to sensitive company information and the verification of employees.
  - **Equipment testing and monitoring:** Companies try to detect incidents and mitigate vulnerabilities through tests, monitoring of the traffic and audits of the infrastructure.

In addition to the GAO study, the White House has initiated some efforts trying to mitigate cybersecurity risks appearing in critical infrastructures including electronic communication networks. In the Executive Order No. 13,636 released in February 2013,[14] the White House calls for NIST to develop a Cybersecurity Framework[15] in order to create a compilation of standards and best practices.

This document represents a guide that can help organizations to improve their own risk management processes and prioritize their cybersecurity decisions. The Framework includes three sub frameworks as described below:

1 – The Framework Core covers a list of cyber security measures that are common around all sectors and industries. These measures are sorted by functions (Identify, Protect, Detect, Respond, and Recover), categories and subcategories. It helps organizations to create or review their security risks management practises and their cybersecurity program taking into account existing standards, guidelines or practises.

[13] GAO (2013), Electronic communication Networks: Addressing Potential Security Risks of Foreign-manufactured Equipment.

[14] Federal Register of U.S.A. (2013), Executive Order 13636—Improving Critical Infrastructure Cybersecurity

[15] National Institute of Standards and Technology (2014), Framework for Improving Critical Infrastructure Cybersecurity.

2 – The Framework Implementation Tiers supports organizations in assessing their own level of security risks management practises. The organization must assess their own performance in a scale which ranges from Partial (Tier 1) to Adaptive (Tier 4).

3 – A Framework Profile: An organization will use the Framework Profile to define their current profile but also the targeted profile they would like to reach in the future including external factors as legal requirements, industry practices, etc. It supports organizations in identifying opportunities for improvement. To make it possible, the organization must use the categories and subcategories previously selected in “The Framework Core” and identify the standards, guidelines and practices that will need to be implemented in order to reach the "targeted objective".

The White House aims with this initiative to alert providers about outsourcing risks. In addition, an organization could use the targeted profile to request its external supplier to adopt specific cybersecurity requirements.

C. India

In March 2010, the Indian Ministry of Communication and Information Technology published new rules on security requirements which should be applied to ICT equipment to prevent and mitigate security threats. However, due to problematic rules such as the disclosure of commercially sensitive source code or the obligation to transfer technology to Indian companies, these requirements suffered from external pressures and were deemed as too restrictive.

In May 2011, the Indian Ministry of Communication and Information Technology decided to present an amended version.[16] According to this amended version, electronic communication service providers should hold the complete and total responsibility of the security of their networks. More specifically, providers must follow strict security guidelines when procuring or outsourcing network elements:

- Providers should have an organizational policy focused on security and security management of their network.
- Providers should audit their network or get it audited by a certified third party from a security point of view once a year in order to assure the resilience and security of it.
- Only network elements tested by relevant contemporary Indian or International Security Standards (ISO, ITU, IETF, IEC...) can be integrated into an Indian network.
- All features, equipment, software, etc., may be subjected to inspection and testing by the Indian Department of Technology at any time.
- Providers should keep records of procedures but also past operation, maintenance, change or update of products.
- Providers should have facilities to detect intrusions, attacks and frauds. Any security breaches must be quickly reported to competent authorities.

To ensure that providers remain compliant, the Indian Department of Technology created a five members committee. Every breach of security will be assessed by the committee which will determine if they have been caused by defects. The electronic communication service providers can be punished with penalties while the suppliers of hardware/software that caused the security issues could be blacklisted, banning them from doing business in the country.

In addition to the mandatory requirements, the Indian Government suggested a list of steps which can be followed by the providers on a voluntary basis. For example, they can create forums or

[16] Government of India Ministry of Communication & IT Department of Electronic communication (2011), Amendment to Unified Access Service License Agreement for security related concerns for expansion of Telecom Services in various zones of the country

associations to increase the security assurance levels and share common issues on the topic. In addition, the government suggested a template agreement[17] which could be signed between the provider and the manufacturer/vendor. In the context of the template agreement, the providers are free to add, modify or delete any clauses to their suit. Main clauses are listed below:

- The vendor must have a well-defined Information Security policy, compliant with ISO/IEC 27001:2005.
- The vendor must be able to demonstrate that they have procedures to deal with security threats.
- The vendor must have a system for detecting and recording any attempted damage, amendment or unauthorised access to provider's information.
- The vendor must be responsible for the software maintenance including upgrades, operating systems and application from factory to desk. Additionally, the vendor shall ensure that software is free of bugs.
- The vendor must ensure that all tools, skills, resources remain operational after the end of the contract.

D. Australia[18]

Since 2012, the Australian government has started considering a reform of its actual electronic communication legislation (The Electronic communication Act (1997)) to include a risk-based regulatory framework. The aim of this framework is to stimulate electronic communication service providers to protect their infrastructure and take into account security risks when making business decisions about the design and development of their network, including when they buy ICT products or outsource ICT services. This approach does not force providers to adopt specific security requirements but educates them on security risks and encourages them to take responsibility over their network security. With it, the Australian government tries to raise providers' awareness about the potential security threats which could happen when developing their infrastructure, taking into account their interactions with vendors.

More precisely, electronic communication service providers should be able to prove their ***competent supervision*** **and** ***effective control*** over their network, either managed in-house or by a third party.

Competent supervision means that providers should be able to watch over their network operations but also over parties which have authorized access to their infrastructure and data such as outsourcing partners or vendors. In addition, it encompasses a reasonable ability to detect security breaches impacting their own services but also compromising the cyber security of the country.

With ***effective control***, providers would need to demonstrate their ability to maintain a direct authority and/or a contractual arrangement over its suppliers, which guarantees the protection of their infrastructure and data from unauthorized access and interference. In that regard, providers would have to request their suppliers monitor and report security issues, as well as to implement preventive actions to mitigate security risks associated with their products or services.

Some compliance assessment and audits may be requested by the government to ensure that providers have the relevant security measures in place to comply with the regulation. In case of unsuccessful compliance, the Australian government has the right to request some mitigation or

[17] Government of India Ministry of Communication & IT Department of Electronic communication (2010), Template of the agreement between Licensee (VSAT & INSAT MSS-R) and vendor of equipment, product and services

[18] Australian Government – Attorney Department (2012), General Equipping Australia against emerging and evolving threats.

remediation actions, including the modification of the infrastructure, audit or ongoing monitoring. In that case, the costs should be supported by provider which would fail to meet the adequate security level requested by the framework. In addition, the government could ask for financial penalties if necessary.

4.1.2 Industry initiatives and International standards

In addition to national frameworks, some industry consortia or organizations have started to develop standards and leading practises to help electronic communication service providers to address the security risks faced when procuring and outsourcing.

When relevant, we map requirements or activities described below to the identified issues experienced by providers described in section 3.

A. ISO/IEC FDIS 27002: Code of practice for information security controls[19]

According to the ISO standards, the security of an organization should not be impacted by the introduction of a third party's product or service. For this reason, ISO/IEC FDIS 27002 includes some security practices used by organizations to manage risks involved in their supplier relationship and take into account the following controls:

1. *Identification of risks related to external parties* (control 6.2.1 – ISO/IEC 17799:2005)

Every time a third party gets access to an organization's information or information processing facilities while offering a product or service, a risk assessment should be performed to determine potential security implications and adequate security requirements that will need to be established by both the organization and the supplier. Among other things, the risk assessment should take into account the following criteria: Type of access granted, targeted facilities, sensitivity of information, identification of persons who get the access, current controls used by third parties, practices to manage security incidents, regulatory requirements, etc.

2. *Addressing security in third party agreements* (control 6.2.3 – ISO/IEC 17799:2005)

All relevant risks and security requirements identified in the previous section (i.e. control 6.2.1) should be incorporated into a contract. This will assure that there is no misunderstanding between the organization and its supplier regarding the security requirements and responsibilities of each party. The contract can be different depending on the organization and the type of supplier used. However, the ISO advises to consider the following terms to be included in each contract:

- Information security objectives to be achieved, as defined by the organization's security policy
- Parties' responsibilities and roles
- Controls to ensure assets protection
- Access control policy
- Change management processes
- Reporting structure and reporting template
- Information security incidents management processes
- Targeted level of service and unacceptable level of service
- KPIs and monitoring process

[19] ISO/IEC International Standard 27002 (2005), Information technology — Security techniques — code of practice for information security

- Right to audit, or to have those audits carried out by a third party
- Service continuity requirements
- Involvement of the third party with subcontractors, and security controls that would be required to be implemented by subcontractors
- Conditions for renegotiation/termination of contract.
- Etc.

3. *Service delivery* (control 10.2.1 – ISO/IEC 17799:2005)

An organization should make sure that the security requirements included in the contract are implemented, operated and maintained by its suppliers (**Issue #3**). In case of an outsourcing relationship, the organization should ensure that the security requirements are maintained also during the transition period, back to the organization or transferred to another supplier.

4. *Monitoring and review of third party services* (control 10.2.2 – ISO/IEC 17799:2005)

An organization should regularly monitor the performance of its vendors by regularly reviewing services reports and records provided by suppliers. In addition, an organization should perform regular audit of its supplier (or involve a third party to perform those audits). Penalties can be used in case of non-compliance with the contract (**Issue #3**).

5. *Managing changes to third party services* (control 10.2.3 – ISO/IEC 17799:2005)

An organization should pay attention to any changes to the provision of services, including changes in security policies, procedures or controls. These changes can be initiated by the organization (e.g. development of new applications, update of policies, etc.) or by its suppliers (e.g. use of new technologies, development of new tools, etc.). In any case, a new risk assessment should be performed to assess new security implications and associated security requirements which should be applied.

In addition to the ISO/IEC FDIS 27002 presented above, ISO organization has recently published a standard (ISO/IEC 27036:2013 – only part 1 and 3 are currently published) related to specific information security techniques applying to supplier relationships.[20] This standard offers further detailed guidance on how to deal with security risks involved in the acquisition of goods and services.

For example, ISO/IEC 27036:2013 advise organizations to adopt a framework with a set of standardized processes for the acquisition of products and services:

- An organization should start by establishing information security and compliance requirements for the exchange of information with the suppliers.
- Before buying or outsourcing, an organization should assess the security risks involved in these processes.
- It should establish a process to negotiate security requirements with the vendors which will be incorporated into the contract (e.g. right to audit, etc.).
- An organization should continuously monitor the performance of its suppliers and refer back to the service level agreement included in the contract in case of deficiencies.

[20] ISO/IEC International Standard 27036 (2014), Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts.

B. Centre for the Protection of National Infrastructure (CPNI): Security Governance Framework for IT Managed Service provision – UK [21]

The Security Framework developed by the CPNI deals with security across the outsourcing process through several elements:

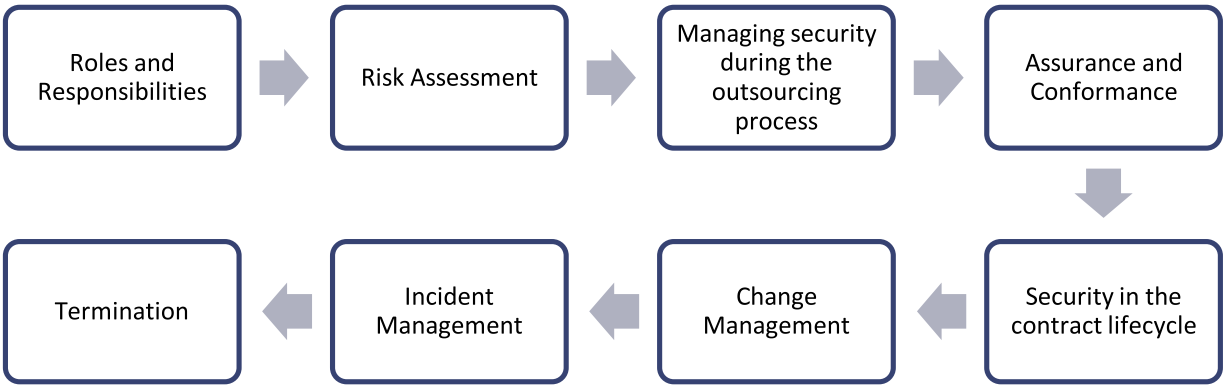
Roles and Responsibilities
Risk Assessment
Managing security during the outsourcing process
Assurance and Conformance
Security in the contract lifecycle
Change Management
Incident Management
Termination

Figure 6: CPNI Security Governance Framework

1. Roles and Responsibilities

When outsourcing, there is a range of key responsibilities that need to be allocated, both at the electronic communication service provider's organization and at the outsourcing partner's organization. More specifically, responsibilities should be established to make sure that security risks and security requirements are clearly articulated and fully understood, that an acceptable level of residual risk is agreed with the provider, that security risks are managed during the complete outsourcing lifecycle, that assurance is gained regarding the security framework in place and that incidents are accurately reported and investigated. These responsibilities should be defined in the contract signed between both parties.

2. Risk assessment

Before starting outsourcing, an organization should assess the security risks involved in this process. To achieve this, an organization should first identify the business processes and functions subjected to outsourcing and the specific governance, regulatory or compliance standards; or other technical constraints which applied to them and could have a security implication.

Then, for each process or function, an assessment should be carried out to evaluate the impact of a loss of confidentiality, integrity or availability on the business. In addition, the organization should assess other security threats such as people/organizations which could attack its systems, their motivation and capacity to do so.

Third, a review of the current and actual vulnerabilities should be performed as well as a review of the current mitigation plans implemented. An organization can always set up a residual risk level which will be accepted by the management. This should nevertheless be in line with the organization's risks appetite.

[21] Centre for the Protection of National Infrastructure (CPNI) (2009), Outsourcing: security governance framework for IT Managed Service Provision

Lastly, the organization should identify the gap between the current level of risk management and the targeted level in order to plan corrective actions.

3. Managing security during the outsourcing process

Once the risk assessment has been performed, an organization has to articulate and develop appropriate security requirements which will be then communicated to the outsourcing services provider. It is crucial for the provider to manage the security during the complete lifecycle of the outsourcing project to ensure that all requirement initially set up are respected by both parties.

Requirements can be set up, communicated, managed and monitored differently based on the organization's security risks management approach:

- The electronic communication service provider can describe in a very detailed manner the controls which will be required to manage security risks. The supplier will then operate its service according to the provider's specifications, developing the technical configurations, procedures, etc. to implement the required controls. The provider will have the right to audit to gain the assurance that controls operate as they should to manage the security risks. This approach will be costly in terms of the provider's resources. Indeed, experts in the fields will be required to specify and negotiate the controls with the supplier. However, it can define exactly how security will be addressed in the outsourcing relationship.
- The electronic communication service providers can also develop a set of high level control objectives (possibly with the help of a third party). If the providers don't do it themselves, it will be the sole responsibility of the supplier to define and implement specific security measures which will meet these objectives. With this approach, the supplier increases its flexibility but needs to provide its customer with the assurance that control objectives have been met.
- Lastly, controls can be setup according to international standards such as ISO 27001/2. In that case, the supplier is required to provide certification of compliance to its client.

The performance of the supplier against the security requirements will be included in the Service Level Agreement. In case of bad performance, suppliers can be subject to financial penalties (**Issue #3**).

4. Assurance and conformance

Organizations which are using outsourcing suppliers should receive assurance from their partners that the risks are correctly managed, that the right processes are in place to guarantee the lowest acceptable level of security risks and ensure that incidents are reported, investigated and corrective actions are taken (**Issue #3**). Assurance can be gained using several methods as agreed in the contract:

- The outsourcing services supplier can report security status and incidents as part of a service reporting;
- The supplier can request regular independent reviews of its systems and report to its customers the results and any corrective actions identified;
- The electronic communication service provider can have the right to audit or the right to review its suppliers' systems. This can also be performed by a third party if needed;
- Assurance can be gained through certification (ISO 27001).

5. Security in the contract lifecycle

Security requirements should stay a priority for the organization using outsourcing services during the complete contract lifecycle.

High level security requirements should be defined even before starting the invitation to tender and request for proposal. This will support the organization in assessing and reviewing its requirements based on suppliers' response and issuing a more detailed statement of requirements later on. The preferred supplier will be selected based on specific security criteria and scoring methods. This means that it has to show its experience and capacity to comply with the security requirements defined by the electronic communication service provider (**Issue#1**).

Once a supplier is selected, both parties enter into the negotiation phase to finalize the contract. This will include the definition of security requirements, the security management approach, the controls specifications and the assurance approach. The contract will be the reference for the supplier to operate the services and manage the risks according to the requirements.

6. Change management

Security risks can evolve and security requirements can become obsolete. So, any contract should take into account potential changes. In addition, the responsibilities for change initiation and additional costs should be established in advance to avoid any further conflict between parties.

7. Termination

Besides, the contract needs to include the procedure to be followed in case of agreement termination. It will help to ensure that the security risks are managed effectively even during the transition from the outsourcing provider back to the customer or another service provider; this includes handling all documents, procedures, configurations etc.

8. Incidents management

The service supplier should report timely and accurately any incidents, near misses or anomalies. Both parties should agree on how incidents should be managed and investigated (**Issue #4**). Third party could be requested to perform the investigation and recommend corrective actions.

C. SAFECode: software Assurance Forum for Excellence in Code[22,23]

The SAFECode association has released several papers to advise software providers in good practices to mitigate security risks involved in their global supply chain.

Commercial software starts to be more and more developed in a global environment, meaning that vendors now serve international markets and use multiple international suppliers to integrate innovative solutions. Each IT product is now a collection of components developed across the globe by several suppliers, their subcontractors or obtained by Open Source repositories.

This global model of distribution raises concerns about additional product security risks and software suppliers are now required to demonstrate the security of the products they produce but also the security of the component they acquire and use. As a result, there is a need to develop a common framework to ensure that the overall software industry address supply chain threats to software integrity (**Issue #6**).

[22] Software Assurance Forum for Excellence in Code (2009), The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain.

[23] Software Assurance Forum for Excellence in Code (2010), The Software Integrity Controls: An Assurance-Based Approach to Minimizing Risk in the Software Supply Chain.

Focusing on Integrity related controls; SAFECode is trying to help organizations in preventing unauthorized or unintentional changes in the source code of the software. SAFECode has developed a range of process guidelines split into three key lifecycle processes:

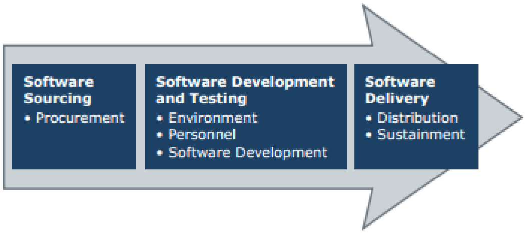

Figure 7: SafeCode Lifecycle Processes

1. Software sourcing process

The controls applied during the sourcing process highly depends on the nature of the relationship between the vendor and it software supplier, and the level of control a vendor has on its supplier. A vendor can set up two main types of controls: contractual integrity controls and technical integrity controls. With the first one, a vendor will sign a written agreement with its supplier clearly stating its expectations, responsibility and ownership of parties, capability of supplier to respond to vulnerability threats and capacity to train its people on evolving secure development practices. On the other hand, technical integrity controls will include more technical requirements such as secure transfer (e.g. encrypted), privileges management, malware scanning, secure storage, secure code exchange.

2. Software Development and Testing

There are different types of controls which can be used to guarantee the integrity of software during the development process. First, an organization should have strong security policy for its people including segregations of duties and security training. Automated processes should always be privileged to minimize the human interventions and decrease the risks from malicious insiders. Second, the environment around the development of the software should be highly secure: the network used and location where the software and code are developed and stored should be secure and have strong access controls. In addition, clear documentation about the change management process, change logs and components/code should be kept for reference in case of issues. Lastly, the organization should test code/software both for vulnerabilities and bugs through automated testing tools but also through manual review to identify common patterns previously identified to ensure that the products function as expected.

3. Software Delivery

In the delivery stage, the software can be delivered directly to the end customers but can also first be delivered to intermediaries such as system integrators, resellers etc. This means that controls falling under this process are similar to the ones developed for the sourcing stage. However, additional security concerns can arise when the product is complete. This brings additional controls such as: final malware scanning, code signing by the software vendor and secure delivery process.

Similarly to the SAFECode initiative described above, the Internet Security Alliance (ISA) has developed guidelines for securing the electronics value chain[24]. More specifically, ISA provides IT companies with very specific security requirements they should apply at each stage of the production of an electronic product. These security guidelines help companies to prevent losses due to interruptions or delay in

[24] The Internet Security Alliance (ISA) (2013), The ISA Guidelines for Securing the Electronics Supply Chain, by Scott Borg.

the production, voluntary or involuntary altered products, discrediting of processes or products, and theft of information/data.

Also, The Open Group Standard developed in 2013 security requirements which would help organizations to mitigate maliciously tainted and counterfeit products[25]. This standard is a set of guidelines, requirements and recommendations built to support vendors in ensuring the integrity of hardware and software developed in a globalized value chain. Such requirements include among other things: physical security procedures, proper access controls, employees' background check, product quality assessment, etc.

[25] Open Group Standard (2013), Mitigating Maliciously Tainted and Counterfeit Products – Version 1.0

5 Security framework commonly used by providers for buying or outsourcing

Following the results of the online survey, the insights discussed during the interviews and the information gathered with the desktop research, it has been observed that many electronic communications service providers have some policy or framework in place to manage the security issues experienced during the procurement or outsourcing of ICT products and services. The security framework usually focuses on the following areas:

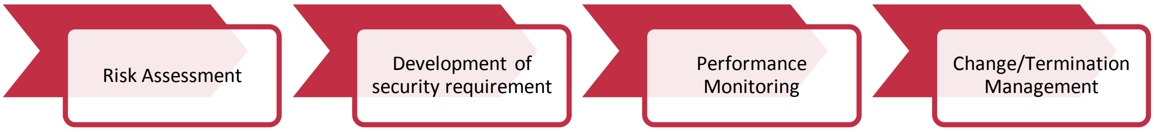
Risk Assessment
Development of security requirement
Performance Monitoring
Change/Termination Management

Figure 8: Framework to address security risks when buying or outsourcing

About 97% of the organizations that participated in the online survey have corporate security policies or security frameworks in place which apply to their relationships with ICT outsourcing partners or ICT products vendors. Among them, 54% apply a different policy depending on the type of products and services procured or outsourced and/or depending on the product and service's criticality. On the other hand, the others seem to apply a standard corporate security policy to mitigate the risks involved in the procurement or outsourcing process.

However, despite the existence of standards related to electronic communication security, providers have highlighted a lack of an integrated and unified approach which will support them in specifically dealing with security risks involved in the procurement and outsourcing process (**Issue #6**). To address this concern, the following sections describe in more details the different steps commonly taken by the providers as identified through the survey to address the security risks involved in the procurement and outsourcing process (See also figure 8).

5.1 Risk Assessment

Several regulators (e.g. Ofcom in the Communication Act 2003) and industry standard consortia (e.g. ISO) advise the electronic communication service providers to perform a Risk Assessment before entering into a relationship with an ICT products vendor or an outsourcing partner. It will help them to identify areas of risks, especially the potential lack effectiveness of vendor's security practises (**Issue #1**), and customize security requirements placed on the vendor accordingly. According to GAO (2013), the providers have the opportunity to take into account the following criteria when performing a Risk Assessment:

- Vendor's actual security practises;
- Vendor's adoption of security standards or industry best practises;
- Vendor's reputation and past performance related to security and resilience of its product/service;
- Information on vendor's subcontractors (e.g. Subcontractors' security policy, reputation, legislation, etc.);
- Criticality of the equipment procured or outsourced (i.e. most critical components require stronger security practises).

The online survey revealed that more than 70% of the respondents use a Network and Information Security (NIS) Risk Assessment before contracting with a vendor. The top risk evaluated through a NIS Risk Assessment is the denial of service attack (figure 9). Most of the respondents scale the denial of service attack as the highest risk due to its direct impact on service availability. The vendors should be able to prove that they have security measures in place to prevent to some extent such incidents to happen, avoiding a complete service collapse for the customers. It is worth noting that Denial of Service attacks represented only a very small percentage of all the outages in the electronic communications services that were reported to ENISA and the Commission in 2012 and 2013[26].

Following the risk of denial of service, the respondents indicated faulty changes/upgrades, bad maintenance and the risk of configuration errors as the risks they would be the most worried about, see figure 9. According to the ENISA incidents report (2013), these risks are relatively common and affect a significant range of providers, and they need to be carefully assessed by the provider. Similarly, the industry associations such as GAO, CPNI, etc., advise providers to assess the vendors' security practises, past performance, reputation, etc., to evaluate the risks of making errors or take faulty decisions.

Lastly, the providers evaluate hardware failures and power cut as part of a NIS Risk Assessment. Those risks are most of the time leading to a complete disruption of service for electronic communication service providers and need to be taken into account. Based on the risk assessments, providers could evaluate the vendors' business continuity and recovery plans used following these kinds of incidents.

The Risk assessment will help providers to evaluate if vendors' security practises are aligned with their own security objectives and would contribute in preventing the security risks they have identified (**Issue #1**). Of course, the existing security framework of the vendor will be improved by additional security requirements set up by the providers to ensure the highest level of security and resilience with electronic communication networks.

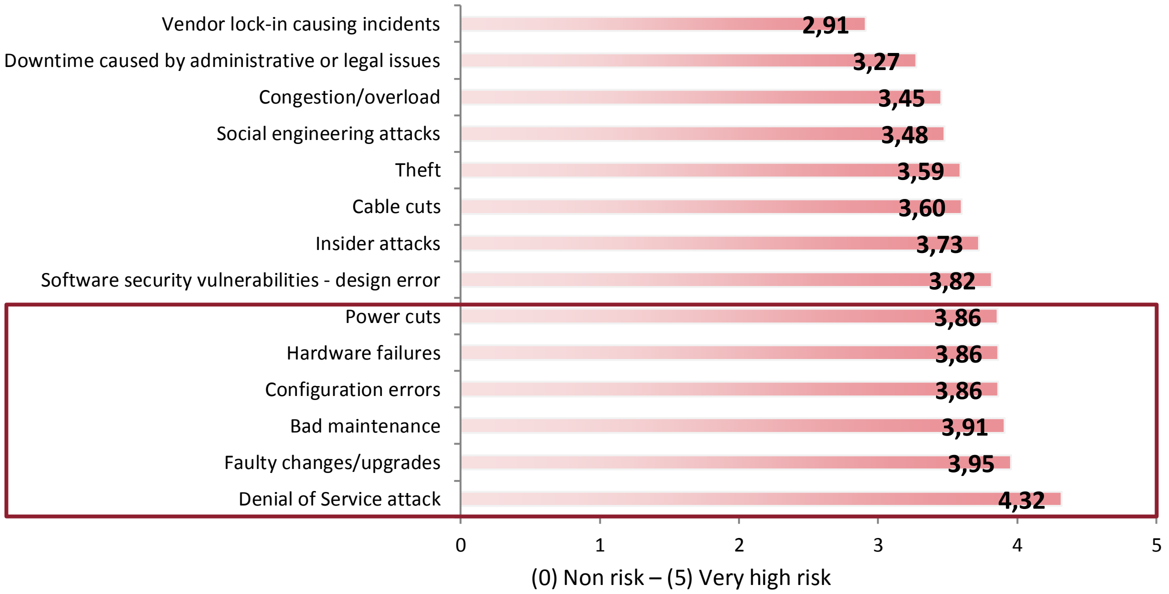

Figure 9: Risks evaluated during a NIS Risk assessment

5.2 Development of Security Requirements

Once the Risk Assessment has been performed, an electronic communication service provider can start to articulate and develop appropriate security requirements which will help them to manage the security risks identified during the Risk Assessment. The security requirements should be

[26] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

implemented by the vendors as agreed with the providers to ensure an on-going and secure delivery of service (**Issue #3**).

According to CPNI (2009), the set-up of high level security requirements could even start before selecting the preferred vendor. High level requirements could be drawn up at the first stage of the vendor's selection process and could be included in the Request for Proposal document in order to select the suppliers based on their capacity to comply with the same and avoid the risk of inefficient security controls (**Issue #1**). Consequently, there is a necessity for each organization to assess and review the capacity of its suppliers through qualifications check and credentials.

The security requirements, together with the clear set of responsibilities of parties, the Key Performance Indicators (KPIs) and the monitoring process should be clearly defined and stated in the contract signed with the vendor. Indeed, providers have highlighted their concern about potential non-compliance of vendors with security requirements defined in the contract (**Issue #3**). Most interviewees agree that the providers have the responsibility to build precise, strong and stable requirements to avoid any confusion or misunderstanding during the whole duration of the relationship with their vendors. The contract will be the reference point for the supplier on how to operate the service and manage the risks according to the requirements. Doing this will ensure a much more smooth and secure process for both parties involved.

"The better you define your criteria, your SLA for example, the better possibilities you have to have a functioning network. As a consequence, the commercial/contractual negotiation phase is key to ensure that realistic and appropriate KPIs are agreed between both parties." [Major equipment vendor]

As part of the contract, 93% of the respondents to the online survey require their vendors to follow certain security requirements. Security requirements are either applied on a case by case basis following a discussion between the relevant stakeholders (technical team, commercial team, architecture team, etc.), or are standardized across the products and services. Only the lower layer products such as switches or routers are mainly subject to more standardized security requirements. The outsourcing services, especially services which demand providers to share confidential data with their vendors, are usually subject to more sophisticated and customized security requirements. During the survey, it has also been cited that security requirements depend on the potential impact of a failure for the customers, so quite naturally, if a product or service breakdown has a significant impact, it will require stronger security requirements.

As per the online survey, 44% of respondents apply different requirements depending on the type of products and services and/or depending on the product/service criticality while the others seem to apply more standardized security requirements to their vendors, for instance in terms of potential user-hours lost.

Overall, the security requirements can vary between different products and services based on:

- The type of product/service provided;
- The criticality of the product and service provided;
- The electronic communication service provider's specific requests or needs;
- The level of resilience of the network;
- The capacity of the network;
- The architecture of the network with a strong focus on redundancies;
- The business continuity/recovery plans in place in case of incidents.

In most cases, setting up security requirements is not particularly challenging as it represents a common practise in the industry. Nevertheless, some providers have expressed their concern about the inherent lack of negotiation power they may have faced with vendors. Some providers expressed that in some cases there could be a non-proportional increase in the costs and the time to market on the vendors' side when requesting additional or too specific security measures (**Issue #5**). Consequently, the providers would need to strongly negotiate with their vendors regarding the level of requirements they want to apply (e.g. actual response time which would be satisfying for the providers).

Most of the security requirements highlighted during the online survey are taken into account by electronic communication service providers when procuring or outsourcing. Nevertheless, it can be observed that all providers do not always apply the same security requirements. On average, each security requirement suggested was either "often applied" or either "applied ad-hoc" by the respondents.

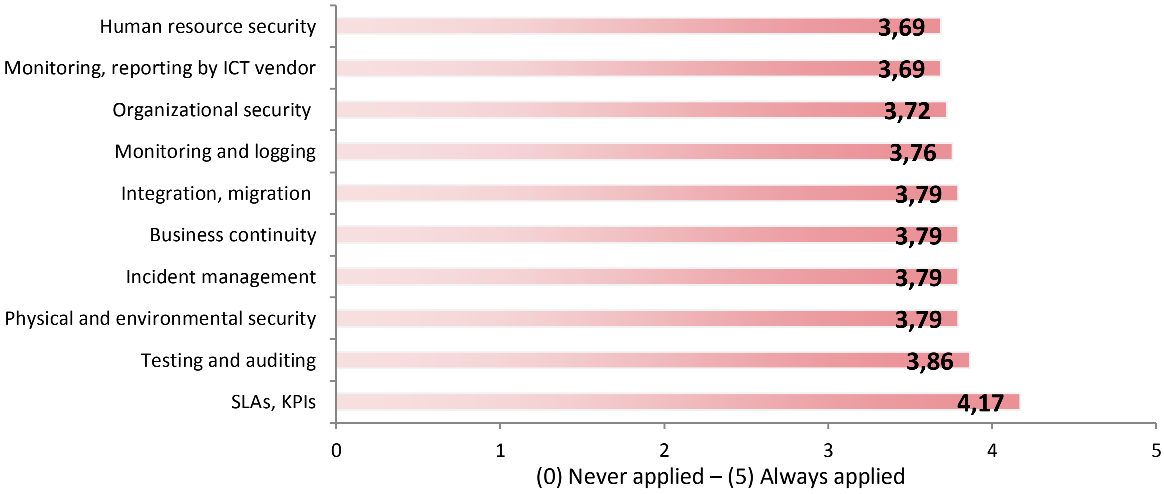

Figure 10: Main requirements from providers applied in the supplier's contract

Overall, the main requirements which providers rely on is the SLA (identified as "always applied"), followed by testing and auditing, see figure 10. Security requirements addressed (and mentioned in figure 10) during the online survey are presented below. Some additional requirements (i.e. assurance, certification and security requirements targeted to subcontractors) have been added due to their importance raised during the desktop research and the interviews.

- **Service Level Agreement and Key Performance Indicators**

The vendor's performance and compliance in regard to contract's security requirements would need to be monitored and compared to a Service Level Agreement (SLA). The interviewees stressed the point that the terms included in the SLA have to be simple, clear and measurable. It is crucial for an electronic communication service provider to be able to verify that the KPIs requirements have been met by the vendor in order to ensure the vendor's compliance with the security requirements set up in the contract (**Issue #3**).

In addition, the provider could develop clear processes to handle any deviations of a vendor regarding the SLA. 76% of providers who responded to the online survey ask for compensation or issue penalties when the performance does not meet the expectations defined in the SLA. Likewise, it has been cited that stronger penalties can help providers to transfer the security risks to the vendors. This means that incidents have a real commercial impact on vendors in order to bring stronger incentives to implement more robust security requirements and take immediate mitigation actions in case of issues.

- **Testing**

It is crucial for a provider to receive the assurance that the products provided or services outsourced are working as they should before integrating them into the existing infrastructure but also along their whole lifecycle. It provides the insurance for the providers that there are not known anomalies or low quality with the product or services procured (**Issue #2**). Hence, testing would need to be performed during the development phase, before and after the integration into the existing infrastructure and when any patches or updates are applied.

Testing can be performed by the vendors, the providers, a third party and/or by collaborative labs. This needs to be agreed during the negotiation phase and included in the contract. As a good practise, complete testing including penetration testing, code review, testing in several environments, iterations testing, etc., should be performed to guarantee the quality of the product and services provided. The vendors are often requested to share testing procedures together with testing results with the provider.

- **Physical and environmental security**

According to SAFECode (2010), the environment around the development of the ICT products and the performance of an ICT service should be highly secure: the network used and location where the equipment and infrastructure are developed and stored should be secure and have strong access controls. In case of physical security breach, malicious attacks could be performed, impacting the integrity of the network and availability of the electronic communications service. In addition, a vendor should ensure that the exchange of information, data or codes is highly secure.

- **Incident management and reporting**

The interviewed providers stressed that the suppliers should report timely and accurately any incidents, near misses or anomalies affecting the electronic communication service providers that happened with their products or services. In some countries such as Australia[27], the suppliers have the obligation to report incidents to the providers.

First, an early warning could immediately be sent in case of anomalies or suspected incidents to inform the provider about the situation and ensure an efficient management of the incident.

Secondly, the vendors could investigate and report in details past incidents or near misses in order to identify causes, learn from the incidents and implement changes when required. A third party could in some cases be requested to perform investigations and recommend corrective actions.

In addition, the vendors could be requested to report to its clients, any incidents which occurred with their products or services across the electronic communication industry. This initiative would increase the transparency regarding potential issues or vulnerabilities and help the providers to prevent the same type of issues.

This initiative has been highlighted many times during the survey meaning that it is crucial for the provider to be informed by the vendor in case there is any problem or a vulnerability is discovered or reported with similar products and services across the electronic communications market (**Issue #2**).

[27] Australian Government – Attorney Department (2012), General Equipping Australia against emerging and evolving threats.

- **Business continuity**

Electronic communications service providers expressed in the interview their concerns regarding potential lack of support from their vendors and outsourcing partners in case of incidents and that their core services will be able to recover quickly (**Issue #4**). Consequently, they are requesting from their suppliers to develop a precise and documented business continuity plan (BCP) and a disaster recovery plan (DRP). During our survey, it was highlighted that providers often define a minimum time for recovery from failure or disaster but also a minimum level of service that should be provided by the vendor (agreed as part of their SLA) in order to ensure the continuity of their critical services or reduce the recovery time. These metrics are usually taken into account by the vendor in the definition of the DRP and BCP.

- **Integration, migration**

Our interviewed providers usually require their vendors to assess the quality and security of the products and services supplied before their integration into the providers' networks. In addition, providers are verifying the quality and functionality of the products against specifications defined in the contract before their integration into their system. Some acceptance criteria can be set up by the provider and the product or equipment can be rejected if it does not comply with the provider's expectations clearly defined in the contract. This will ensure that products and services are working as they should and avoid any unexpected anomalies (**Issue #2**).

However, quality and security are not only critical during the integration of a product or a service into the provider's network. It should be managed and ensured also in case of upgrade or decommission. The change management process should indeed include accurate and efficient testing to guarantee the security and quality during any change.

- **Organizational security**

Providers in our survey are often concerned that vendors' security controls would not be aligned with their own security objectives and would fail to prevent the security risks they have identified (**Issue #1**). According to ISO/IEC FDIS 27002 standards, the security of an organization should not be impacted by the introduction of third party products or services. Therefore, the suppliers could adopt the security policy of their client or have a security policy aligned with the electronic communications service provider's security objectives in order to provide them with the same level of security they apply in-house.

- **Monitoring and logging**

It has been highlighted many times during the survey that the monitoring of vendors' products is crucial for a provider. One of their concerns is a lack of monitoring and logging from their vendor regarding potential security breaches, unauthorized accesses or unauthorized changes which could occur with their products or services. Vendors have the opportunity to increase the security level by monitoring and logging for issues and breach and share critical information with providers to increase the resilience of electronic communication services.

- **Human resources security**

Among the queried security requirements, human resource management was the least applied among the providers. Vendors have the opportunity to increase the quality of their services by providing valuable technical knowledge and skills to the providers. To achieve this, it is crucial for vendors to have highly trained and knowledgeable staff, capable to support providers in their technical request and guide them in ensuring a high level of resilience. This is even more important when dealing with incidents or disaster. Many times, providers have raised concern regarding potential bad support from their vendors in case they have to recover their network following an incident (**Issue #4**).

- **Assurance**

The interviewed providers raised that assurance should be provided by the vendor that security risks are managed continuously and that requirements are implemented and operated as agreed with the electronic communication service provider in the contract (**Issue #3**). Assurance can be gained using several methods which should be defined in the contract[28]:

- The supplier can regularly report the security status and incidents as part of a service reporting.
- The supplier can request regular independent reviews of its own systems and reports the results and any corrective actions identified to its customers. In that case, the supplier supports the costs associated with the audit or inspection. This approach requires no financial investment from the electronic communication service provider.
- The electronic communication service provider can have the right of audit or the right of inspection of its suppliers' systems. Audits and inspections represent a big investment and are costly measures for the providers. Nevertheless, most of the providers include in the contract the right to audit or inspect their supplier's infrastructure as this represents a very useful tool for ensuring compliance and keeping with agreed standards. However, the decision to perform an audit is made on a case by case basis, depending on the context and the criticality of the product or service provided. About 66% of the providers who answered to the online survey perform (or request 3rd parties to perform) audits of their vendors and outsourcing partners.
- Assurance can also partly be gained through certification (e.g. ISO 27001).

- **Certifications**

Certifications are often required by the surveyed providers for the outsourcing partners (ISO 2700x, ISA 3402). It provides the provider with an independent assurance that the vendor's controls have been correctly designed and operate effectively (**Issue #1**). According to the online survey, 62% of respondents request specific products or services certification from their vendors.

- **Subcontractors' requirements**

Due to the globalization of the ICT products supply chain, more and more players are now interacting to produce a single product. As a result, some of the electronic communications service providers take into account potential subcontractors of their vendors when developing security requirements. According to the ISO/IEC FDIS 27002 standard, the security requirements applying to the main vendors should also be imposed to downstream suppliers. In addition, a provider should always verify the methodology used by its vendors to select and manage their own suppliers.

5.3 Performance Monitoring

An organization has the opportunity to continuously monitor the performance of its vendors in order to assess the compliance of the vendors with security requirements set up in the contract (**Issue #3**). To facilitate the monitoring, it is crucial that vendors share all the information, data, record and knowledge indispensable for the electronic communication service providers to monitor their

[28] Centre for the Protection of National Infrastructure (CPNI) (2009), Outsourcing: security governance framework for IT Managed Service Provision

performance. Performance should be assessed against the KPIs defined in the SLA and corrective actions or penalties can be applied in case of deficiencies. Examples of main KPIs used are

- Uptime
- Response time to alarms
- Issues resolution time

Some providers are using a collaborative approach when dealing with security risks involved in the procurement and outsourcing process. It involves a strong collaboration between parties in terms of sharing of information and sharing of knowledge which supports the electronic communication service providers in testing and monitoring the performance of the vendor's products and services. Indeed, some interviewees expressed that in many cases, the providers need to have better information about the products and services provided to accurately monitor the performance of their vendors.

5.4 Change/Termination Management

According to CPNI (2009), the security risks can evolve and the security requirements can quickly become obsolete. Consequently, the provider together with the vendor could discuss and plan how to handle any future changes in security requirements. More importantly, processes for change management and responsibilities regarding change initiation would need to be established in advance and included in the contract. Both parties can also define who will support the cost depending on the type of change and include the same in the contract.

In addition, the contract needs to include the procedure to be followed in case the agreement is terminated. This will ensure that the security risks are managed effectively even during the transition from the outsourcing supplier/vendor back to the customer or another supplier. The termination process includes:

- Transferring all documents, procedures, configuration, record, etc. relating the product or service to the electronic communication service provider to ensure a smooth continuation of it;
- Handling to the electronic communication service provider or destroying all documents, files, records containing provider's information;
- In case the retention of some information is agreed with the provider, specific security measures need to be agreed and implemented to ensure the confidentiality and the protection of the data.

6 Recommendations

Based on concerns expressed by providers, our own observations and existing initiatives, we provide in this section a set of general recommendations to the sector and specific recommendations to providers that could be taken to improve the security of electronic communication networks and services with respect to dependencies on third party products and managed services. The aim of these recommendations is to support the management of security risks faced by providers when buying ICT products and services and contribute to an appropriate level of security and resilience.

In parallel with this report we are publishing a separate Security Guide aimed at providers and also vendors, where we propose guidance on specific security requirements providers may request from their vendors when entering into a contractual relationship.[29]

6.1 General recommendations to the electronic communications sector

The following two general recommendations are aimed at Member States and the actors in the electronic communications sector.

Recommendation 1: Member States should promote the awareness about security risks related to ICT procurement and outsourcing

Member States must ensure that the introduction of third party's products or services into an electronic communication network does not impact the level of resilience and thus the continuity of supply of services for the customers. There is a need to raise awareness with providers and vendors about the importance of managing security risks involved in the procurement and outsourcing of ICT products.

Applying security requirements to vendors will help providers to comply with Article 13a and address the security and integrity of their networks and services. Member states, in particular NRAs, have the opportunity to stimulate the development of security practises targeted to the procurement and outsourcing but also the sharing of best practises, knowledge, and tips and tricks between electronic communications service providers on dealing with ICT vendors. This will support the industry to develop a more unified and integrated approach which will support providers in specifically dealing with security risks involved in the procurement and outsourcing process (**Issue #6**).

Recommendation 2: Vendors, providers and critical customers should develop a collaborative approach to defining security requirements, to sharing information about security vulnerabilities and threats, and to the mitigation of incidents

Providers often procure similar ICT products and they often have similar security requirements. This means there is an opportunity for providers to collaborate and jointly set security requirements. The ENISA security guide for ICT procurement could be used as a basis for such collaboration.[30]

The vendors of ICT products and services should collaborate with providers in order to build more resilient and secure electronic communication services for end customers and for the whole society. This should start in the beginning of the procurement or outsourcing process as it helps the provider and the vendor to jointly define clear, actionable and measurable security requirements and avoid disputes going forward (**Issue #3**). The ENISA Security Guide for ICT Procurement could be used as the basis for such security requirements.[31] The security requirements become a reference point for the supplier on how to manage the risks during the complete lifecycle of the relationship. And because

[29] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
[30] Ibid.
[31] Ibid.

security risks can change over time, and new issues might come up, there should be a mechanism which allows vendors, providers and critical customers (e.g. within the energy, health, and transport sector respectively), to share information in case of discovered vulnerabilities, threats, near-incidents and incidents (**Issue #2)**.

Lastly, the vendor can support providers in monitoring and testing the performance of procured products and outsourced services, and the providers should receive appropriate and prompt support by the vendors in case of problems or occurred security incidents (**Issue #4)**.

As highlighted during the survey, by adopting a more collaborative approach, vendors, providers and users will all benefit from a more transparent view and in the end more resilient networks and services.

6.2 Recommendations to individual providers of electronic communications networks and services

The following recommendations are specifically aimed at providers of electronic communications networks and services.

Recommendation 3: Engage internal stakeholders and develop a holistic risks management approach

When addressing security risks in the procurement and outsourcing process, the electronic communications service provider should involve stakeholders *across* the organization (**Issue #2, #3, #4**). The ENISA Security Guide for ICT Procurement[32] could be used as a starting point for working with internal stakeholders (e.g. the information security team, procurement team, architecture team and the management team).

It is particularly important to ensure that these security practises are embedded in the whole organisation. There needs to be procedures in place for addressing and developing vendor security requirements between network and security experts, procurement and not least management.

Recommendation 4: Conduct a risk assessment before procuring or outsourcing to third party

Before starting the procurement or outsourcing process and entering into a relationship with a third party, the electronic communications service provider is advised to conduct a Risk Assessment. A Risk Assessment will support the provider in better identifying the security risks they may face if they enter in such a relationship, especially the potential lack effectiveness of vendor's security practises (**Issue #1**), and develop specific and relevant security requirements targeted to the vendor which will prevent or mitigate those risks. Security Risks Assessment can include (but is not limited to) the following elements:

- Criticality of the product procured or service outsourced;
- Potential impact in case of loss of confidentiality, integrity or availability;
- Known and identified vulnerabilities;
- External security threats such as malicious attacks;
- Minimum level of residual risk which is acceptable by the electronic communication service provider;
- Vendor's existing security practises including internal security practises, adoption of security standard or recognised industry practises, etc.;
- Vendor's past performance or reputation on past performance;
- Ability to change vendors (in order to avoid vendor lock-in);

[32] Ibid.

- Information on vendor's subcontractors.
- Vendor's financial status (e.g. credit worthiness, solidity, etc.).

Recommendation 5: Develop high level security policy and requirements before selecting preferred vendor

The provider should define their own high level security policy for third-party procuring or outsourcing. High level security requirements could already be developed at the beginning of the selection process and more precisely when writing the request for proposal. Indeed, this will help the provider to only consider suppliers based on their capacity to comply with the same and avoid the risk of inefficient security controls (**Issue #1**). With this leading practise, the provider can expect saving time and money when evaluating their possibilities in terms of vendors. All the same, they have to assess and review the capacity of its suppliers through qualifications checks and credentials.

Recommendation 6: Develop clear, solid, measurable and actionable security requirements for vendors

The provider should develop and define clear, simple, measurable and actionable security requirements, for specific ICT products or services, in order to facilitate their implementation by the vendor and avoid any confusion or misunderstanding during the contract lifecycle (**Issue #3**). The ENISA Security Guide for ICT Procurement[33] can be consulted for this purpose. It is advised to develop solid security requirements which will not require further significant changes. Changes in security requirements risk weakening the vendor's security practises and bringing confusion in the relationship.

Recommendation 7: Prioritize the implementation of the security requirements for vendors

Depending on the type and criticality of the products or services, different security requirements and different levels of security are needed. One size does not fit all. Criteria from regulatory requirements as well as internal criteria such as uptime, number of users affected in case of failure etc. should be considered to give security requirements a proper prioritization. This allows stakeholders inside the organization to focus on the most important requirements first.

Recommendation 8: Manage security risks through the procurement lifecycle

Efforts to ensure sufficient levels of security should be carried out through the project lifecycle and not only during the vendor selection process. Different steps should be in place to guarantee integrity, confidentiality and availability of the services throughout the product or service lifecycle. For example, testing could be performed in the development phase of the product/system, before its integration in the provider's infrastructure, along its lifecycle and after each patch or update.

Recommendation 9: Monitor the performance of your vendors

The provider should continuously monitor the performance of their vendors by regularly reviewing service reports and records provided by the later, or other means such as audits or technical inspections. Performance can be assessed against the KPIs defined in the SLA and corrective actions or penalties can be used in case of deficiencies. Higher penalties can be applied for highly critical systems, and by doing so, vendors may be more risk aware about the provider's core services and the role their products and services play. This will support the provider in ensuring the compliance of its vendor with security requirements defined in the contract (**Issue #3**).

[33] Ibid.

References

Related ENISA papers

- ENISA (2014), Security Guide for ICT Procurement https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors
- ENISA (2014), Annual incident reports 2013 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013
- ENISA (2014), Technical Guideline on Security Measures (Version 2.0) https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures

Legislation

- Australian Government – Attorney Department (2012), General Equipping Australia against emerging and evolving threats. http://apo.org.au/research/equipping-australia-against-emerging-and-evolving-threats
- Federal Register of U.S.A. (2013), Executive Order 13636—Improving Critical Infrastructure Cybersecurity. https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
- Government of India Ministry of Communication & IT Department of Electronic communication (2010), Template of the agreement between Licensee (VSAT & INSAT MSS-R) and vendor of equipment, product and services
- Government of India Ministry of Communication & IT Department of Electronic communication (2011), Amendment to Unified Access Service License Agreement for security related concerns for expansion of Telecom Services in various zones of the country
- HM Government (2013), Huawei Cyber Security Evaluation Centre: Review by the National Security Adviser. https://www.gov.uk/government/publications/huawei-cyber-security-review
- National Institute of Standards and Technology (2014), Framework for Improving Critical Infrastructure Cybersecurity. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- Ofcom (2012), Ofcom guidance on security requirements in the revised Communication Act 2003: Implementing the revised EU Framework.
- Ofcom (2014), Updating Ofcom’s guidance on network security.
- Ofcom (2014), Ofcom guidance on security requirements in sections 105A to D of the Communication Act 2003. http://stakeholders.ofcom.org.uk/telecoms/policy/security-resilience/

Others

- Booz Allen Hamilton (2012), Managing Risks on Global ICT Supply Chains: Best practises and standards for acquiring ICT http://www.boozallen.com/media/file/managing-risk-in-global-ict-supply-chains-vp.pdf
- Centre for the Protection of National Infrastructure (CPNI) (2009), Outsourcing: security governance framework for IT Managed Service Provision http://www.cpni.gov.uk/Documents/Publications/2006/2006027-GPG_Outsourcing_IT.pdf

- GAO (2013), Electronic communication Networks: Addressing Potential Security Risks of Foreign-manufactured Equipment.
  http://www.gao.gov/assets/660/654763.pdf
- Infonetics (2013), “Telecom equipment vendors manage 45% of the world’s subscribers as outsourcing grows” viewed on http://www.infonetics.com/pr/2013/1H13-Service-Provider-Outsourcing-Market-Highlights.asp 01/14/14
- ISO/IEC International Standard 27002 (2005), Information technology — Security techniques — code of practice for information security
  http://www.iso.org/iso/catalogue_detail?csnumber=50297
- ISO/IEC International Standard 27036 (2014), Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts.
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=59648
- NIST (2013), Supply Chain Risk Management Practices for Federal Information Systems and Organizations.
  http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf
- Open Group Standard (2013), Mitigating Maliciously Tainted and Counterfeit Products – Version 1.0
  https://www2.opengroup.org/ogsys/catalog/c139
- Software Assurance Forum for Excellence in Code (2009),The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain.
  www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf
- Software Assurance Forum for Excellence in Code (2010), The Software Integrity Controls: An Assurance-Based Approach to Minimizing Risk in the Software Supply Chain.
  http://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf
- The Internet Security Alliance (ISA) (2013), The ISA Guidelines for Securing the Electronics Supply Chain. By Scott Borg
  http://isalliance.org/publications/9B._ISA_Guidelines_for_Securing_the_Electronic_Supply_Chain-Phase_III_Document-Scott_Borg.pdf
- The Register, “O2 outage outrage blamed on new Ericsson database” viewed on http://www.theregister.co.uk/2012/07/13/o2_outage_cause

TP-07-14-065-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN: 978-92-9204-116-8
DOI: 10.2824/094009

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu