Security Guide for ICT Procurement

ICT Procurement Security Guide for Electronic Communications Service Providers

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 Communications 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, Genséric Cantournet).

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

ISBN: 978-92-9204-117-5, DOI: 10.2824/994989

Executive summary

The goal of this Security Guide for ICT Procurement is to support primarily electronic communications service providers but also ICT vendors with practical guidelines to better manage potential security risks in procured products or outsourced services which could lead to disruptions or outages in electronic communications services.

In this Security Guide we map a set of security risks with security requirements which can be applied to vendors to prevent or mitigate those risks. The described risks and proposed security requirements are based on findings from a desk top study, a questionnaire with 29 providers and interviews with 10 providers and 2 vendors.

We hope that the Security Guide for ICT Procurement will be useful for providers when negotiating and collaborating with ICT product vendors or outsourcing partners and for vendors when developing and managing the security of their portfolio of products and services.

Table of Contents

1 Introduction

Entering into a relationship with vendors for purchasing key ICT products or outsourcing managed services for core operations can expose an electronic communications service provider and primarily its customers to security risks leading to, but not limited to, intentional or unintentional incidents impacting the continuity of electronic communications services. In order to prevent or mitigate such security risks, providers have the opportunity to apply specific security requirements to their suppliers or outsourcing partners.

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 those relationships. For this reason and in cooperation with providers in the ENISA Electronic Communications Reference Group ENISA has studied this topic and developed this Security Guide for ICT Procurement that providers but also vendors may use when entering into a contractual relationship regarding products and outsourced services for core operations of electronic communications networks and services.

Goal and Scope

With this report ENISA's objective is to support primarily electronic communications service providers but also ICT vendors with practical guidelines to better manage the security risks impacting the resilience of networks and services.

More specifically, it provides an overview of the security risks to be considered when procuring critical ICT products or outsourcing critical ICT services to third parties. This report examines the risks in third party products or services which could lead to the disruption of the electronic communications services for the customers, and the report equips providers with specific and practical security requirements aimed at vendors in order to prevent or mitigate such security risks, to better deal with them in the procurement or outsourcing phase and avoid or recover from breaches in their core services.

Target audience

The Security Guide for ICT Procurement is primarily targeted at providers and its experts responsible for and involved in the procurement of key ICT products and services. It will support the providers in the definition of security requirements which will be applied to their vendors and outsourcing partners to guarantee the resilience and security of their networks and services. In addition, it can be used by vendors in the development and security management of their products and services. This will help them in meeting the expectations of the providers at the early phase of the procurement process.

Methodology

In order to gather experience and opinions from experts in the field, ENISA has:

- launched an anonymous online survey to providers across the EU bringing insights from 29 providers about their main concerns and areas of focus when buying ICT equipment or outsourcing ICT services to third parties, 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;
- performed interviews with experts from 10 providers and 2 vendors, from several countries within Europe but also companies from other countries, and

- performed a desktop research and analysed initiatives already taken by Governments, National Regulatory Authorities (NRAs) and the industry including guidelines shared by providers and vendors.[1]

By analysing these inputs, specific security requirements have been drafted, which could be applied by vendors to ensure the security and resilience of electronic communication networks and services.

The findings from the survey, issues and concerns that providers have expressed, current applied practices, our own observations, general recommendations to the sector as well as recommendations to the providers, are all summarised in a separate report called *Secure ICT Procurement in Electronic Communications*.[2]

Structure of this document

To stay consistent with ENISA's Technical Guideline on Security Measures Version 2.0, and in line with recommendations received from the interviewees, the Security Guide is structured according to ENISA's seven security domains (D1-7).[3]

D1: Governance and risk management
D2: Human resources security
D3: Security of systems and facilities
D4: Operations management
D5: Incident management
D6: Business continuity management
D7: Monitoring, auditing and testing

In section 2 the report maps the identified security risks to be addressed in the procurement or outsourcing process, to security requirements which can be applied to the vendors to prevent or mitigate those risks.

[1] See references, page 22.

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

[3] Note that security requirements in this Security Guide are specifically addressed to vendors in their role as suppliers of products or services for core operations of electronic communications networks and services, and they should not be mixed up with the security measures described in the ENISA Technical Guideline on Security Measures (v 2.0), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures

2 Security requirements for vendors

The security requirements in this Security Guide for ICT Procurement are based on ENISA's survey with providers and vendors and on guidelines shared by providers and vendors, and they are also inspired by good practises promoted by industry standards or by country regulated initiatives.

Please note that throughout this document "provider" refers to electronic communications network and service providers while "vendor" refers to suppliers of ICT products or outsourcing partners.

These guidelines have been divided in the seven security domains and split across the 25 security objectives (SO) defined in ENISA's Technical Guideline on Security Measures Version 2.0.[4] For each security objective we describe one or several risks, and mapped to the risks we propose a set of security requirements aimed at vendors.

2.1 Governance and risk management

SO1: Information security policy/ SO2: Governance and risk management

Security Risks
Vendor's failure to align its security practises to the provider's security objectives.
Security requirements
✓ The provider's security objectives should be fully understood and integrated by the vendor. ✓ The vendor selected should have an information security policy ensuring the security and resilience of its products and services, and aligned with the provider's high level security objectives. ✓ The vendor should provide evidence of its relevant internal information security policy ensuring the security and resilience of its products and services for provider's analysis.
Security Risks
Vendor's failure to meet the provider's security objectives due to a lack of communication and misunderstanding between the two parties regarding actions to be taken by the vendor.
Security requirements
✓ A contract should be signed by the vendor enforcing specific security requirements, defined by the provider and aligned with its security objectives. Security requirements should be clear, precise, actionable and measurable. ✓ Security requirements are defined by the provider during the Risk Assessment. ✓ The provider should be able to request updates on the security requirements in light of any tests/exercises or incidents affecting the provider's systems and/or the vendor's similar products or services in the electronic communications sector. Updated security requirements would then be implemented undisputedly by the vendor.

[4] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures

Security Risks
Provider's failure to comply with national legal obligations imposed by law or secondary legislation due to lack of support from the vendor.
Security requirements
✓ The provider should be able to request the vendor to comply with legal obligations imposed by law or secondary legislation on the provider without any increase of costs.

SO3: Security roles and responsibilities

Security Risks
Failure to clearly and/or correctly establish key roles and responsibilities regarding security risks management between the provider and the vendor leading to: - Confusion and misunderstanding between parties in case of a threat or incident; - Incorrect implementation of security requirements; - Lack of accountability in case of security breaches not recognised within the vendor's organization.
Security requirements
✓ Clearly define and state responsibilities and roles within the contract to avoid confusion, misunderstanding or abuses. ✓ One person within the vendor's organization should be accountable during the whole contract lifecycle to ensure that: - security risks and requirements are fully understood; - appropriate processes are in place and a minimum acceptable level of residual risk is agreed with the provider and duly accepted by each party; - security risks are managed and appropriate processes are in place and communicated to the provider; - Appropriate support is provided to the provider through relevant helpdesk or other as defined by the contract; - Contractual clauses are respected. ✓ Force Majeure which releases the vendor from its responsibility should be clearly defined to avoid any abuses from the vendor.

SO4: Security of third party assets

Security Risks
Provider's exposure to additional security threats due to the vendor's use of downstream subcontractors to provide products or services to the provider. These threats include but are not limited to: - Lack of information regarding the downstream subcontractors; - Lack of vendor's competent supervision and effective control on its subcontractors; Failure to enforce security requirements to the vendor's subcontractors.
Security requirements
✓ The vendor should provide information regarding existing and/or potential subcontractors used to provide products and services to the provider. This information will be included in the Risk Assessment performed by the provider and should be taken into account in the definition of the security requirements. ✓ The subcontractor must comply with the same or equivalent security measures as the ones applied to the vendor. ✓ The vendor should remain solely accountable for all the actions performed by its subcontractors, responsible for managing security within its subcontractors and providing assurance that security requirements operate efficiently to meet the provider's security objectives.

2.2 Human resources security

SO5: Background check

Security Risks
Unintentional or intentional alterations of products or systems performed by the vendor's employees including faulty changes or upgrades, configuration errors, bad maintenance, insider attacks, etc.
Security requirements
✓ Credentials of the vendor's employees should be provided to demonstrate their relevant experience in security risks management. ✓ When legally permitted and justified by a level of criticality of service provided, the vendor should do its due diligence to flag any criminal records in its employees' background, to avoid any sinister and intentional alterations of products or systems. Evidence of the due diligence should be made available to the provider for consultation.

SO6: Security knowledge and training

Security Risks
Vendor's failure to allocate sufficient skilled and trained resources to effectively and efficiently manage security risks.
Security requirements
✓ The vendor's employees' should receive appropriate training to implement and operate security requirements applied by the provider. ✓ The vendor should provide sufficient evidence regarding the training program of its employees. ✓ If requested by the provider, the vendor should have the required qualified personnel (e.g. ISO certified). ✓ A designated proportion of the vendor's employees should follow regular training to stay up-to-date in an evolved technological environment with changing security practises. ✓ The vendor should provide sufficient evidence regarding the training program of its employees. ✓ The vendor should carry out its due diligence to ensure that its employees have sufficient security and technical knowledge, skills and qualification, to avoid any unintentional alterations of products or systems. Evidences of the due diligence should be available to the provider for consultation.

SO7: Personnel changes

Security Risks
Disrupted and inefficient management of security risks due to entry or change of personnel on the vendor's side with deviations from the contract specifications.
Security requirements
✓ All personnel from the vendors or downstream subcontractors, who are given access to confidential information or customer personal data related to the provider, should sign a confidentiality or non-disclosure agreement with their employer. The vendor should also have clauses regarding confidentiality and personal data protection included in the contract signed with the provider. ✓ Any change of personnel, as defined and agreed in the contract, should be mentioned to the provider. ✓ Any replacements of personnel in the scope of the service should be agreed with the provider. ✓ A knowledge transfer process should be defined and executed by the vendor between the employees that get substituted. ✓ Access right to the provider's information systems should be timely revoked by the vendor for personnel who have been discharged.

2.3 Security of systems and facilities

SO9: Physical and environmental security

Security Risks

Unintentional or intentional alteration of products or systems due to weak or a lack of physical access measures provided by the vendor.

Natural phenomenon's impacts (Overheating, storms, floods, etc.) on products or systems due to weak or a lack of physical security measures provided by the vendor.

Security requirements

- ✓ The vendor should have specific security processes in place ensuring the physical security of its products or systems, and preventing any unauthorized access to its physical facilities and infrastructure including but not limited to:
  - Procedures for securing manufacturing sites;
  - Procedures for securing storage sites;
  - Procedures for securing operational sites;
  - Procedures for securing the packaging and the transport of equipment.
- ✓ Evidence of the physical security processes should be shared with the provider for analysis.
- ✓ Processes should be followed routinely by the vendor.
- ✓ The effectiveness of the processes should be periodically assessed by the vendor and revised when required, especially following any incidents and tests/exercises affecting the provider's systems and/or the vendor's similar products or services in the electronic communications sector.

SO11: Access control to network and information systems

Security Risks
Unintentional or Intentional alteration of products or systems due to weak or a lack of logical access measures provided by the vendor.

Security requirements

- ✓ The vendor should have specific logical access controls in place ensuring the security of its products or systems and preventing any unauthorized access to its networks and information systems: including but not limited to:
  - User identification and authentication;
  - Unique ID;
  - Segregation of duties;
  - Privilege based access groups.
- ✓ Evidence of logical access controls should be shared with the provider for analysis.
- ✓ The effectiveness of the processes should be periodically assessed by the vendor and revised when required, especially following tests/exercises or any incidents affecting the provider's systems and/or the vendor's similar products or services in the electronic communications sector.
- ✓ Access to sensitive networks and information systems should be restricted to the vendor's employees who have a specific business need.
- ✓ Access list with the vendor's individuals authorized to access networks and information systems with their rights and privileges should be regularly reviewed by the vendor.
- ✓ A review of activity log should be performed by the vendor in order to flag any anomalous behaviour. This review should be performed by a third party (e.g. independent quality reviewer within the vendor organization).
- ✓ Systems detecting and recording any attempted damage, amendment or unauthorized access should be implemented by the vendor.
- ✓ Note that these last 2 measures are relatively costly and severe to implement for a vendor. It could be requested only in case highly critical provider's information systems are involved.

SO12: Integrity of network and information systems

Security Risks
Insertion of malicious content such as viruses, code or malware leading to an alteration of the integrity and/or the functionality of a product or a system.
Security requirements
✓ The vendor should validate the product's or system's integrity by performing appropriate scanning and testing before its integration into the provider's infrastructure. ✓ Testing/Scanning procedures and results should be shared with the provider for analysis. ✓ In case of counterfeit items, the vendor should take the appropriate measures to replace it, ensuring the continuity of service for the provider with the same level of security.

2.4 Operations management

SO13: Operational procedures

Security Risks
Vendor's failure to run its daily operations according to the provider's security requirements.
Security requirements
✓ As part of the contract, the vendor should agree with the provider on a Service Level Agreement (SLA) that specifies, in measurable terms, what services the vendor shall provide. This includes: – The minimum level of service that the provider will accept. – The minimum level of residual risk (once controls have been implemented) that the provider will accept. This minimum acceptable level of residual risk should be agreed with the provider's senior management. – Security oriented Key Performance Indicators (KPI) under which the provider will assess the vendor's performance. KPIs should be precise and measurable. ✓ The vendor's performance will be regularly assessed and the provider will refer back to the SLA. ✓ The vendor should provide any supportive data, record or report which will facilitate the assessment of its performance by the provider. In addition, the vendor should share the knowledge necessary for the provider to fully understand the data, record or report. ✓ The vendor should be exposed to penalties in case of insufficiencies or divergences with the SLA. For highly critical systems, higher penalties should be agreed.

SO14: Change management

Security Risks
Failed changes (e.g. update failure) leading to partial or complete disruption of services for the providers due to lack or inefficient change management processes. Inefficient security requirements due to weak or lack of change management processes in an evolving environment with constant technological changes.
Security requirements
✓ The vendor should maintain processes for change management. A different process can be implemented based on the type of change required: - Newly discovered vulnerability leading to adoption of additional security measures; - Software update; - Hardware replacement. ✓ The change management process should include accurate and efficient testing (see SO 23). More precisely, the vendor should test any software or hardware changes before its integration into the life environment. Evidences should be provided to the provider. ✓ The responsibilities for the change initiation and the additional cost payment should be established in advance and stated in the contract. ✓ The vendor should take responsibilities for changes related to: – Any vendor initiated changes; – Other changes agreed in the contract (e.g. update). – Variations in the service levels caused by the vendor; – Newly discovered vulnerabilities in vendor's product or system; ✓ Vendor's corrective actions following a security incident.

Security Risks

Vendor's failure to maintain a suitable security level and operate security requirements during the transition process once the contract with the provider is terminated.

This includes the transition from the vendor back to the provider or to another vendor.

Security requirements

- ✓ A contingency plan should be in place in case either party wishes to terminate the relationship even before the end of the agreement.
- ✓ The vendor should define and agree with the provider on a transition plan ensuring the management of security until the handover to the provider or to another vendor is completed.
- ✓ The vendor should transfer all documents, procedures, configuration, records, etc. related to the product or service which are necessary to guarantee a smooth continuation of the service for the provider.
- ✓ The vendor should return or destroy all files, records, documents 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 by the vendor to ensure the confidentiality and the protection of the provider's data.

SO15: Asset management

Security Risks

Lack of timely replacement plan and efficient logistic function in case some components, products or systems break sooner or become obsolete making the replacement* or update** of an element impossible, and leading to a disruption of service for the provider.

*Vendors may discontinue the production of some of their products as technology advances very fast. Components, products or systems can be unavailable for a provider. A replacement will not be possible.

** As technology advances very fast, an update can be incompatible with an obsolete system or infrastructure. An update will not be possible.

Security requirements

- ✓ The vendor should maintain processes for change management (e.g. software update, hardware replacement, etc.) (see SO14).
- ✓ The vendor should consider the time frame within which its products or systems are expected to become obsolete.
- ✓ The vendor should perform regular checks on its products and systems to detect any early signs of obsolescence.
- ✓ A replacement or updating plan should be developed and implemented by the vendor taking into account the availability of compatible products, spare parts and compatible updates with the existing infrastructure to ensure the continuity of services for the provider.
- ✓ The vendor should provide the evidence that it has an efficient logistic function managing the inventory of its components, products and systems and ensuring the availability of them or conformed substitutes in a reasonable time.
- ✓ The vendor should warrant the replacement or updates of any critical components, products or systems in the timeframe agreed with the provider in the contract in order to avoid any breach of services for the provider (Refer to SO19).
- ✓ The vendor should notify the provider when a product's update is available.
- ✓ Support should be provided by the vendor in case of replacement or update.
- ✓ The minimum time for which the product will be supported by the vendor should be agreed by both parties as part of the contract.

2.5 Incident management

SO16: Incident management procedures

Security Risks
Extended impact of a disruption of service due to an inefficient management of incidents.
Security requirements
✓ The vendor should have an emergency procedure in place to deal with incidents and/or provide support to the provider to manage incidents. The procedure will include scenarios per type of incidents, parties' roles and responsibilities, escalation process, etc. ✓ The vendor should have a service continuity plan (see SO19) and a disaster recovery plan (see SO20) in place to minimize the impact of an incident on the provider's service availability. ✓ The vendor should comply with the mean time to repair and mean time to recover defined in the SLA and agreed with the provider. ✓ Each incident management case should be evaluated by the vendor and a report should be available for the provider (see SO18). ✓ If required for improvement of the incident management procedure, some enhancement actions (e.g. better workflows, new ways of contact, etc.) could be agreed with the provider and implemented by the vendor (see SO18).

SO18: Incident reporting and communications

Security Risks

Failure to send timely early warning to inform the provider about any anomaly, suspected incident or suspected near miss leading to a bad incident management and disruption of service.

Lack of information regarding past incidents, suspected incidents, near-misses, suspected near misses or anomalies occurring within the provider's infrastructure.

Security requirements

- ✓ Processes should be implemented by the vendor to accurately and timely report to the provider any security incidents and security breaches occurring with its products or services, or any data breaches related to the provider, as well as any violations of security requirements stated in the contract or required by law.
  - The vendor should immediately raise an early warning in case of anomalies, suspected incidents or suspected near missed;
  - The vendor should report any past incidents, suspected incidents, near-misses, suspected near misses or anomalies occurring within the provider's infrastructure.
- ✓ Some thresholds could be set up with the agreement of the provider to report only specific alarms based on their criticality.
- ✓ The vendor should also report to the provider, any incidents which occurred with its products or services across the electronic communications industry (i.e. impacting other providers), when that same products and services are also contracted by the provider.
- ✓ A clear escalation process should be established between the vendor and the provider to ensure a well-defined and efficient communication flow. It should define escalation channels and contacts (primary and backup contacts) between both parties.
- ✓ The vendor should investigate, support provider in the investigation or request a third party to investigate past incidents to find the root causes. This can be agreed in the contract or on a case by case basis.
- ✓ If required to avoid further incidents, corrective actions could be agreed with the provider and implemented by the vendor.

2.6 Business continuity management

SO19: Services continuity strategy and contingency plans

Security Risks
Weak or lack of service continuity strategy defined to guarantee the availability of service for the provider in case of an incident.
Security requirements
✓ The vendor shall ensure by tools, skills, resources or processes that services of the provider remain operational at all times, complying with the minimum level of service defined in the SLA and accepted by the provider. This can include, i.a.: – Spare parts[5] – Back up – Back up personnel to ensure critical functions are always maintained ✓ The vendor should provide complete documentation of business continuity processes. ✓ More specifically, the outsourcing service vendor should have a service continuity plan with a strong emphasis on potential failures of power supplies. This is very significant given that a failure of the power supplies can lead to a complete interruption of service for the provider. ✓ The vendor's business continuity plan should consider its dependencies of subcontractors ✓ The vendor should review its service continuity plan based on past incidents and past experience and revise it if necessary.

[5] A duplicate part to replace a lost or damaged part of a machine.

SO20: Disaster recovery capabilities

Security Risks
Weak or lack of service recovery capabilities to restore the service of the provider in case of disaster, major outage or complete interruption of service.
Security requirements
✓ The vendor shall ensure by tools, skills, resources or processes that services of the provider can recover from a major incident within the minimum time for recovery defined in the SLA. This can include, i.a.: – Spare parts[6] – Back up – Back up personnel to ensure critical functions are always maintained ✓ The vendor's recovery plan should consider its dependencies of subcontractors ✓ The vendor should review its service recovery plan based on past incidents and past experience and revise it if necessary. ✓ If requested by the provider, the vendor could take part to a drill with the provider to prepare them in potential big disruptions (storms, huge disaster, individual disruptions of critical network equipment, etc.).

2.7 Monitoring, auditing and testing

SO21: Monitoring and logging policies

Security Risks
Undetected abnormal performance, bugs or malicious actions due to inefficient traffic or equipment performance monitoring.
Security requirements
✓ A constant monitoring should be performed by the vendor to detect any abnormal activity that may indicate issues related to availability or integrity of the provider's network and system. ✓ Any anomalies should be investigated by the vendor. ✓ Any anomalies should be immediately reported to the provider (refer to SO18).

[6] A duplicate part to replace a lost or damaged part of a machine.

SO23: Network and information systems testing

Security Risks
Inadequate, ineffective or insufficient testing leading to vulnerabilities, malfunctions or other failures of vendor's products and services.

Security requirements
✓ Quality and security of the product should be assessed by the vendor against specifications defined in the contract before its integration into the provider's 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. The process is valid for new components, patches and update. ✓ The vendor should do its due diligence to ensure regular, accurate and efficient testing and provide the assurance that products and services are operating as they should: - Testing should be performed along product/service lifecycle: from the development stage, before and after its integration to the existing network and when any patches or updates are performed; - Testing should be made with the right configuration - in the testing environment, simulating life environment configurations (or substitute) when feasible ; - Testing should be made by iterations to allow the vendor to apply fixes when required; - Several types of testing should be performed including but not limited to known vulnerabilities scans, penetration testing, source code analysis, etc. ✓ Testing can be performed by the vendor, the provider, a third party and/or by a collaborative lab (with provider's and vendor's testers). Parties accountable for the testing need to be agreed and stated in the contract. ✓ Testing frequency needs to be agreed and stated in the contract. ✓ Testing plans and methodologies should be regularly reviewed based on, technology changes, upgrades and past incidents. ✓ The vendor should share a comprehensive testing report which shall include testing procedures, identified vulnerabilities, any mitigating actions required and a clear escalation process in case of further issues.

SO24: Security assessments

Security Risks
Insufficient information about products' or systems' potential vulnerabilities before selecting a vendor or a supplier of outsourcing services. Weak preventive actions implemented to face the same.
Security requirements
✓ Before entering into a relationship, the vendor should provide its client with documentation on known products' and systems' potential vulnerabilities together with their criticality and likelihood of being exposed. ✓ A process should be implemented by the vendor to promptly notify the provider about any newly discovered and exploitable vulnerability (refer to SO18). ✓ The vendor should take into account the evolving threats landscape and should periodically review the industry security alerts/standards to assess any new potential vulnerability.

SO25: Compliance monitoring

Security Risks

Failure to gain assurance regarding the vendor's compliance with the security requirements and failure to ensure that security risks are correctly managed by the vendor. For example:

- Controls not in place;
- Controls in place not aligned with the provider's security objectives;
- Deviation in controls.

Security requirements

- ✓ Regular meetings should be organized between the vendor and the provider to assess the performance of the vendor regarding the application of the security requirements.
- ✓ The assurance should be provided by the vendor that the security risks are managed and the requirements are implemented and operate as agreed with the provider in the contract. Parties should agree on the scope, the methodology and the frequency of the assurance report. The assurance can be gained using several methods:
  - The vendor can report the security status, risks, vulnerabilities and incidents, as part of a service reporting.
  - The vendor can request regular independent reviews of its service or production processes and facilities, and reports to the provider the results and any corrective action identified. Note that this measure is costly for the vendor so it is generally applied on a case by case basis.
  - The provider can have a right of audit or a right of review of its vendor's service or production processes including equipment, software, information, record, data or person relating to it. This can also be performed by a third party if needed. Note that this measure is costly for the provider so it is generally applied on a case by case basis.
- ✓ Assurance can be gained through certification (e.g. ISO 27001).

References

Related ENISA papers

- ENISA (2014), Secure ICT Procurement in Electronic Communications 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-05-14-129-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: 978-92-9204-117-5
DOI: 10.2824/994989

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