NISDUC

NIS Directive User Community

D3.2: NISDUC Lessons learnt – vol.2

Co-financed by the European Union
Connecting Europe Facility

Project acronym	NISDUC
Project title	NIS Directive User Community
Start date of the project	01/09/2020
Duration	36 months
Funding instrument	Connecting Europe Facility: Telecom (CEF Telecom)
Call for proposals	CEF-TC-2019-2 – Cybersecurity
Objective	Objective 4: Trans-European cooperation for effective joint cybersecurity operations and to build mutual trust/confidence
Agreement number	INEA/CEF/ICT/A2019/2072562
Action No	2019-EU-IA-0129

Deliverable type	Report
Deliverable reference number	D3.2 / V1.0
Activity contributing to the deliverable	Activity 3: Monitoring on the practices and experiences of the implementation of the NIS Directive
Due date	29/04/2022
Dissemination level	Public
Revision	V1.0

Contributors (ordered according to beneficiary numbers and alphabetical order of first names)

Hervé Cholez, Jocelyn Aubert, Nicolas Mayer (**LIST**)

Guy Mahowald, Pascal Bertrand, Sheila Becker, Joao Filipe Dos Santos (**ILR**)

Albert Jorissen, Philippe Faccinetto, Pierre-François Vandenhaute, Rudi Smet, Tim Masy (**BIPT-IBPT**)

Gérard Wagener (**SECURITYMADEIN.LU**)

Reviewers

Caroline Breure (**CCB**)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the authors’ views – the European Health and Digital Executive Agency (HaDEA) is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Table of contents

Lessons learnt from a collaborative approach involving Operators of Essential Services (OES), the National Competent Authority (NCA) and the Single Point of Contact (SPOC)

This section proposes best practices and experiences in the deployment of the NIS Directive based on a collaborative approach involving regulated entities (OES) and regulation authorities (NCA and SPOC).

These practices refer to actual implementations of the NIS Directive in Luxembourg and Belgium, established by, for Luxembourg, the **Institut Luxembourgeois de Régulation (ILR)**, the NIS identified SPOC, the NCA for the DSPs and for OES (except for banking and the financial market infrastructure), and, for Belgium, the **Belgian Institute for Postal services and Telecommunications (BIPT)**, the NIS sectoral authority for Digital Infrastructures in Belgium, both assisted by the **Luxembourg Institute of Science and Technology (LIST)**, a mission-driven Research and Technology Organization that develops advanced technologies and delivers innovative products and services to industry and society.

Incident notification thresholds definition approach

This sub-chapter explains how in Luxembourg, the criteria to notify incidents are defined and established, so that the national competent authority and the OES are aligned in terms of incident notification and, therefore, make collaboration with the involved actors more efficient.

For each sector, there are various criteria to determine if an incident must be reported to the national competent authority or not. These criteria can be split into two categories: the sector specific criteria and the non-sector specific criteria.

The non-sector specific criteria are not linked to the availability of the essential service, but to the impact of the incident, to e.g.:

- The user death risk or health.
- Society aspects like e.g., the security, the public safety…
- Financial and material aspects.
- Data confidentiality, integrity, and availability.

The sector specific criteria can consider:

- The unavailability of the essential service through e.g., the estimation of the number of impacted users and the duration of the impact.
- The components necessary to the availability of the essential service.

Concerning the definition of the notification criteria, on one hand, the non-sector specific ones are defined by the national competent authority and applied to any sector. On the other hand, the sector specific ones, as well as their thresholds, are defined jointly with the operators. The thresholds are selected in such a way, that an everyday insignificant incident would not lead to an incident notification but would still be sensitive enough to detect as soon as possible any unusual behaviour and critical situation and have the possibility both for the operator and the national competent authority to swiftly react to it.

Data analysis

As part of the adoption of the NIS Directive [1] in Luxembourg, a security risk management framework has been established. This approach covers the entire regulatory cycle, meaning three successive steps: the processing of security risk management by the regulated entities (i.e., OES), the gathering and analysis of risk-related data by the regulation authority (i.e., the NCA), and finally the improvement for the next cycle of the whole framework based on lessons learnt from the previous steps.

The approach relies on a structured risk methodology to be followed by OES, as well as sector-*specific models produced following the approach described in NISDUC Lessons learnt – vol.1 [2]. Such models make possible to define both a common language and a minimum scope for the risk assessments, by defining concepts to be used, including primary assets, supporting assets, risks to be considered, but also scales for assessing risk scenarios in particular likelihood and impact. Based on the standardised analyses produced by the OSE, the NCA can therefore analyses the situation of individual operators in detail as well as obtain an overview of the risks for the concerned sector and the whole ecosystem.*

To facilitate the work of analysing the results, a complete data analysis framework has been developed. The purpose was therefore to define:

- A set of measurements **depicting the trust the NCA can have in the security of OES**, as well as in the different sectors. The outcome for the NCA is to be able to provide recommendations to the OES and facilitate policymaking.
- A set of measurements **intended for OES**, to enable them to better perceive their level of exposure to risks and their own level of protection.

The first task when defining the measurement framework was to establish a template for the measurement constructs, inspired by the state of the art, and in particular the recommendations suggested by ISO/IEC 27004 [3]. Then, once the measurement template was established, two types of measurements were defined: compliance measurements, measuring compliance with requirements imposed by legislation, and effectiveness measurements, measuring the effectiveness of risk management and security, and classified in three main categories, namely:

- **Risk Effectiveness**: measuring the security risk management effectiveness.
- **Security Maturity**: measuring the information security maturity, relying on the sophistication levels proposed by ENISA.
- **Risk-Maturity Gap**: comparing Risk Effectiveness with Security Maturity, to assess the consistency of the risk management activities compared to the security maturity stated.

The final sets obtained are composed respectively of 125 measurements for the NCA, and 60 measurements for OES. For the sake of brevity, the detailed lists of measurements are available in Annex I (p.15) and Annex II (p.19).

Measurement set for the NCA

The measurement set for the NCA should allow the following:

- Analyse the security level of a specific OSE for a specific year (based on a specific risk assessment report) with:
  - General information on the **report** (including report quality level, differentiation from the previous report).

    - General information on the **risks considered** in the report (including average risk levels, risks summary, unacceptable risk ratio, etc.).
    - Detailed information on the **risk concepts** used within the report, as well as rankings of the risk concepts leading to the main identified risks.
    - An overview of **Security Objectives distribution** for the OSE.
    - A detailed analysis of the **coherence between the governance of information security and the perceived levels of risk**, helping to identify consistency/inconsistency between declared maturity and a subset of risks targeting specific security domains.

- Analyse the evolution of the security level of a specific OSE (based on numerous risk assessment reports) with:
    - General information on **risks evolution** (including evolution of average risk levels, comparative risk summary, etc.).
    - Detailed information on the **evolution of risk concepts** used within different reports of the OSE, as well as evolution of rankings of the risk concepts leading to the main identified risks.
    - An overview of the **evolution of Security Objectives distribution**.
    - A detailed analysis of the **evolution of the coherence between the governance of information security and the perceived levels of risk**.

- Analyse the security level of a specific sector, considering several OSE from this sector for a specific year (based on specific risk assessment reports) with:
    - General information of the **reports** (i.e., the number of received/missing reports).
    - General information on **risks considered** in the reports (including average risk levels, risks summary, unacceptable risks ratio, etc.).
    - Detailed information on the **risk concepts** used within the reports, as well as rankings of the risk concepts leading to the main identified risks.
    - An overview of **Security Objectives distribution** for the OSE.
    - A detailed analysis of the **coherence between the governance of information security and the perceived levels of risk**, helping to identify consistency/inconsistency between declared maturity and a subset of risks targeting specific security domains.

- Analyse the evolution of the security level of a specific sector, considering several OSE from this sector (based on numerous risk assessments reports) with:
    - General information on **risks evolution** (including evolution of average risk levels, comparative risk summary, etc.).
    - Detailed information on the **evolution of risk concepts** used within different reports of several OSE, as well as evolution of rankings of the risk concepts leading to the main identified risks.
    - An overview of the **evolution of Security Objectives distribution**.
    - A detailed analysis of the **evolution of the coherence between the governance of information security and the perceived levels of risk**.

Measurement set for the OSE

The measurement set for the OSE should allow the following:

- Analyse the OSE security level for a specific year (based on a specific risk assessment report) with:

  - General information on the **risks considered** in the report (including average risk levels, risks summary, unacceptable risk ratio, etc.).
  - Detailed information on the **risk concepts** used within the report, as well as rankings of the risk concepts leading to the main identified risks.
  - An overview of **Security Objectives distribution** for the OSE.
  - A detailed analysis of **the coherence between the governance of information security and the perceived levels of risk**, helping to identify consistency/inconsistency between declared maturity and a subset of risks targeting specific security domains.

- Analyse the evolution of the OSE security level (based on numerous risk assessment reports) with:
  - General information on **risks evolution** (including evolution of average risk levels, comparative risk summary, etc.).
  - Detailed information on the **evolution of risk concepts** used within different reports of the OSE, as well as evolution of rankings of the risk concepts leading to the main identified risks.
  - An overview of the **evolution of Security Objectives distribution**.
  - A detailed analysis of the **evolution of the coherence between the governance of information security and the perceived levels of risk**.

Lessons learnt from Computer Security Incident Response Teams (CSIRTs)

Automation

With the increase of security incidents and the complexity of infrastructures, automation helps to perform some tasks more efficiently. The advantages are already discussed in the deliverable D3.1-NISDUC Lessons learnt vol.1 [2]. The open-source community is continuously trying to improve data sharing software such as MISP [4], IntelMQ [5] frequently used in the CSIRT community. To increase automation within the CISRT community in Europe, DG-CNECT launched the tender SMART 2014/1079 on 16th September 2014 to collect the requirements [6]. This tender was won by Deloitte who delivered reports including requirements. The outcome was that in the CSIRT community a heterogeneity of systems with different maturity levels are used.

Standards like STIX [7] try to address the interoperability of common data format and language. However, there are often cases that cannot be properly encoded in standard formats. TAXII [8] defines a RESTful API that can be implemented by client and servers to ease automation. However, the challenge with TAXII is to integrate it in old legacy incident handling software used by CSIRTs and their constituents such as network operators or abuse teams. Examples of such software are JIRA [9], OTRS [10], and RTIR [11].

In the tender SMART 2015/1089 [12], DG CNECT awarded it to a consortium led by Capgemini to develop a toolbox of software available for the CSIRT community. The core idea was that each CSIRT used the same software to ensure interoperability. The maintenance and testing of each software component was cumbersome and did not scale regarding vulnerabilities in included software packages or the software itself of MeliCERTes.

On the 13th of May 2019, DG-CNECT published another tender called SMART 2018/1024 [13] to maintain the MeliCERTes platform. The contract was awarded to a consortium led by NASK.pl[1] who are also in the CSIRT network [14] via CERT.pl. CIRCL is also in this consortium and the MeliCERTes platform is being based on the Cerebrate software [15]. CIRCL leads the development of this software. The consortium switched to a lighter deployment model where each CSIRT has the autonomy of management of its own software. Cerebrate focuses on the orchestration of various tools. The advantage of Cerebrate is that it can be opened to a broader community. Initially for the CSIRTs but is also designed to be used by ISAC (Information Sharing and Analysis Center) and SOC (Security Operations Center) to ease automation between CSIRTs up to SOC or ISACs within their constituency. Cerebrate might be a candidate for competent authorities in NIS to orchestrate data sharing, risk assessment tools used between OES and DSPs and the competent authorities. DG CNECT launched on 31st of May 2019 a tender called SMART 2018/1023 [16] to build a platform for the NIS cooperation group.

The last mile towards SOCs and ISACs can be still improved. Some OES and DSP manage their own networks and have set the descriptions of RIPE objects such as the network name or abuse contacts. As contacts are either email addresses given often generic email addresses of NOC (Network Operation Centre) or abuse teams. Each organization has its own process to handle the received

[1] Naukowa i Akademicka Sieć Komputerowa ("*Research and Academic Computer Network*" in Polish) is a Polish research and development organization and data networks operator.

notification. Some processes are manual some automated or semi-automated. Some OES are behind a third-party network owner. CIRCL is promoting MISP for the data sharing and automation. However, due to the heterogeneity of processes and systems with its customized configuration, interoperability is often not granted even when both entities use automation. DG CNECT launched new funding schemes from 2021-2027 in their Digital programme [17] that could be used to improve on these topics.

Voluntary data sharing aspects

Notification has a cost. It is composed of the processing cost, the identification time to find a responsible person to take some actions, the follow up etc. CSIRTs are notifying constituents regarding security vulnerabilities, compromised systems, or leaked data. The concept of PSIRT (Product incident response teams) [18] emerged such that vendors have dedicated resources to handle vulnerabilities in their products. Nevertheless, there are many vendors that do not have these capacities. The identification of a person in such an organization is already a tedious task to receive the notification. The fix of the vulnerability remains a business decision of the vendor. There are many vulnerabilities that are never fixed. Other organizations offering services, such as Internet access, must have an abuse contact in their respective RIPE objects. The processing of these abuse messages is bound due to business decisions: from semi automating abuse messages to ignoring them. The implementation of GDPR lead to that WHOIS information was not accessible to the public any-more [19]. An OES has its infrastructure behind and network owner ignoring abuse requests never gets the information that his server is compromised from CSIRTs or security researchers. Hence, a voluntary approach could be used to interconnect the various entities. The Cerebrate software could be used to share contact details about automation systems such as MISP server URLs.

Lessons learned from telecom sector for the implementation of NIS 2 proposals relative to the supervision and control

Telecom framework

In 2009, the European Union introduced obligations in terms of security by means of Directive 2009/140/EC [20].

This Directive lays down the following, among other things:

- undertakings providing public communications networks or publicly available electronic communications services **take appropriate technical and organisational measures** to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.
- undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus **ensure the continuity** of supply of services provided over those networks.
- undertakings providing public communications networks or publicly available electronic communications services **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.

These obligations have been supplemented and made permanent by Directive 2018/1972 [21].

It should be noted that these obligations apply to all entities in the electronic communications sector, without restrictions based on the type of the services provided or the size of the operators.

These obligations strongly influenced the proposal introduced by the Commission in December 2020 to adapt the Directive on the security of networks and information systems.

In Belgium, it should also be mentioned that the entities providing electronic communications services must notify the designated national authority[2]. Furthermore, the Directive on the protection of critical infrastructure also applies to the electronic communications sector.

Heterogeneity of the telecommunications sector

The heterogeneity of the telecommunications sector is due to the following factors:

- The different types of customers.
- The wide range of services.
- Global players covering different countries.
- The geographic spread.

Regarding the analysis in terms of societal security, it is essential to note that the operators' customers are very different. Certain customers are essential to the functioning of society and others are not. The security of a service may be vital for a customer and not for another customer, for instance, a 112-

[2] https://www.bipt.be/operators/notifying-the-bipt

emergency call centre or a hospital's broadband access in comparison with an internet access of a retail customer.

The telecommunications sector mainly provides these services to two big market segments: retail and B2B. Different services are offered in each of these segments. Concerning retail, we can mention broadband access, voice services (number-based or not) and a multitude of value-added services. Concerning B2B, we can mention the supply/concession of cables and fibre or the provision of corporate communications services to an undertaking with the assignment of numbers by using extension services for private networks.

The size of the operators, particularly in terms of capitalisation, turnover or number of customers, is very different. Certain players are active at the local level, and others at the national and/or global level. The undertakings' organisational structures and business models are also very different from one operator to the other.

Failure of the one-size-fits-all supervision approach in the telecom sector

When one wishes to apply a supervision in terms of security in such a heterogenous sector, it is impossible to implement a one-size-fits-all approach. Regarding regulation, the principle of proportionality of the measures is to be observed. Therefore, imposing preventively several days of audit to players with no activity that is important for the proper functioning of society is unacceptable. The reverse is also true. Not auditing players who are vital to our daily lives is equally unacceptable and could threaten our way of life.

It is therefore valid to note the failure of the one-size-fits-all supervision approach.

Failure of the isolated supervision approach in the telecom sector

The institutional authorities can no longer ensure, single-handed, the security, particularly since the privatisation of various vital sectors, such as the electronic communications sector.

It should also be noted that the private and public entities are no longer able to ensure their security on their own. Technological developments force them to call on human resources, hardware, software or data from third parties to ensure their security. Moreover, the increasing number of threats and their increasing intensity, particularly hybrid state threats on civil installations, require cooperation among the various players to close the gap between the resources of the attackers and their defences, notably by pooling their resources.

It is also necessary to be able to rely on a reliable and redundant supply chain.

Similar conclusions can be drawn regarding the sector regulation models. The supervision resulting from these models can now only rely on the competences and goodwill of an individual authority. On the one hand, the obvious dependencies among sectors lead to collaboration needs among public institutions and also between public and private institutions. On the other hand, the various threats and risks require particular competences such as the gathering of information, technical knowledge and know-how, legal powers fragmented among various public and private entities.

It is therefore necessary to note the failure of an isolated approach of the supervision of entities.

Possible way of working in the telecom sector: collaborative systemic risk-based approach

Based on the elements set out above, the preferred approach in the telecommunications sector is:

- A step-by-step approach: the supervision in terms of security should be adapted to the regulated entity based on the associated risks.
- A systemic approach: the supervision should consider the dependencies of the regulated entities to other entities but also of other entities to the regulated entities, thus their suppliers as well as their customers. Furthermore, the supervision should be based on various factual information such as risk analyses, incidents, audits, threat assessments.
- A collaborative approach: the supervision should lead to information sharing between public and private actors, among other things.

The Luxembourgish approach

In Luxembourg, the transposition of the NIS directive appointed the NRA in the Telecom sector as competent authority for the following sectors: Energy, Transport, Health, Drinking water supply and distribution and Digital Infrastructure. The NRA is as well competent regarding the Articles 40 and 41 of the EECC [21]. It therefore could use its experience gained in the Telecom sector for the sectors of the NIS Directive.

The operators of essential services have the obligation, like the telecom operators, to notify on a yearly basis, their technical and organizational measures to manage risks in relation with their network and information systems which they use in their operations.

This is done via the transmission of two types of information:

- **A list of security objectives**, where the operators indicate to which extend, they have implemented the security objectives. These objectives are based on ENISA's Guideline on Security Measures under the EECC [22]. Since they are linked to the security of Network and Information Systems, they can also be used for the Network and Information systems of the operators of essential services.
- **A risk assessment**, the operators of essential service should update on a yearly basis. The risk assessment is based on the ISO/IEC 27005 [22] and ISO/IEC 27001 [24] standards. For the Telecom sector, the NRA has set up with a Research and Technology Organization (LIST), a platform, where the operators could perform their risk assessment. This platform is also used for the operators of essential services.

In regard to the NIS 2 proposal, to regroup the different sectors in one directive, including the telecom sector, has the advantage that the requirements for the different sectors will be more streamlined and the use of common platform and common security objectives and guidelines will make the supervision and control much easier and benchmarking between sectors will become an additional asset to assess the maturity of the different sectors in relation to the security of their network and information systems.

Annex I: Measurement set for the National Competent Authority

Measurements to analyse the security level of a specific OSE for a specific year (based on a specific risk assessment report)

General information on reports	Overall report quality level
	Differentiation from the previous report
General information on risks	Overall average risk level
	Average risk level for a specific service (resp. primary asset)
	Average risk level for a specific supporting asset
	Overall current risk levels distribution
	Current risk levels distribution for a specific service (resp. primary asset)
	Overall estimated residual risk levels distribution
	Estimated residual risk levels distribution for a specific service (resp. primary asset)
	Overall risk summary
	Unacceptable risks ratio
	Unacceptable risks ratio for a specific service (resp. primary asset)
	Overall average risk level of unacceptable risks
	Average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	List of supporting assets associated to a specific service (resp. primary asset)
	List of threats considered for a specific service (resp. primary asset)
	List of vulnerabilities considered for a specific service (resp. primary asset)
	List of controls considered for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest current risk level
	Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest estimated residual risk level
	Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Top 10 vulnerabilities the most exploited
	Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Top 10 most targeted supporting assets
	Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Top 10 security measures
Security objectives	Sophistication levels breakdown
	Security Objectives ranking by sophistication level
	Security Objectives sophistication level per SO
	Security Objectives sophistication level per domain
Maturity / Risk management ratios	Maturity / Risk management ratio (physical and environmental security)
	Maturity / Risk management ratio (technological security)
	Maturity / Risk management ratio (human resources security)
	Maturity / Risk management ratio (Incident management & contingency plan)
	Maturity / Risk management ratio (Operational security)

Measurements to analyse the evolution of the security level of a specific OSE (based on numerous risk assessment reports)

General information on risks	Evolution of overall average risk level
	Evolution of average risk level for a specific service (resp. primary asset)
	Evolution of risk level for a specific supporting asset
	Comparative overall risk summary
	Evolution of unacceptable risks ratio
	Evolution of unacceptable risks ratio for a specific service (resp. primary asset)
	Evolution of the overall average risk level of unacceptable risks
	Evolution of the average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	Evolution of Top 10 threats leading to risks with the highest current risk level
	Evolution of Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Evolution of Top 10 vulnerabilities the most exploited
	Evolution of Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Evolution of Top 10 most targeted supporting assets
	Evolution of Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Evolution of Top 10 security measures
Security objectives	Evolution of sophistication levels breakdown
	Evolution of Security Objectives ranking by sophistication level
	Evolution of Security Objectives sophistication level per SO
	Evolution of Security Objectives sophistication level per domain
Maturity / Risk management ratios	Evolution of Maturity / Risk management ratio (physical and environmental security)
	Evolution of Maturity / Risk management ratio (technological security)
	Evolution of Maturity / Risk management ratio (human resources security)
	Evolution of Maturity / Risk management ratio (incident management and contingency plan)
	Evolution of Maturity / Risk management ratio (operational security)

Measurements to analyse the security level of a specific sector, considering several OSE from this sector for a specific year (based on specific risk assessment reports)

General information on reports	Number of received/missing reports
	Overall average risk level

General information on risks	Average risk level for a specific service (resp. primary asset)
	Average risk level for a specific supporting asset
	Overall current risk levels distribution
	Current risk levels distribution for a specific service (resp. primary asset)
	Overall estimated residual risk levels distribution
	Estimated residual risk levels distribution for a specific service (resp. primary asset)
	Overall risk summary
	Unacceptable risks ratio
	Unacceptable risks ratio for a specific service (resp. primary asset)
	Overall average risk level of unacceptable risks
	Average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	List of supporting assets associated to a specific service (resp. primary asset)
	List of threats considered for a specific service (resp. primary asset)
	List of vulnerabilities considered for a specific service (resp. primary asset)
	List of controls considered for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest current risk level
	Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest estimated residual risk level
	Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Top 10 vulnerabilities the most exploited
	Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Top 10 most targeted supporting assets
	Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Top 10 security measures
Security objectives	Sophistication levels breakdown
	Top 5 Security Objectives with the highest sophistication level
	Top 5 Security Objectives with the lowest sophistication level
	Security Objectives sophistication level per SO
	Security Objectives sophistication level per domain
Maturity / Risk management ratios	Maturity / Risk management ratio (physical and environmental security)
	Maturity / Risk management ratio (technological security)
	Maturity / Risk management ratio (human resources security)
	Maturity / Risk management ratio (Incident management & contingency plan)
	Maturity / Risk management ratio (Operational security)

Measurements to analyse the evolution of the security level of a specific sector, considering several OSE from this sector (based on numerous risk assessments reports)

General information on risks	Evolution of overall average risk level
	Evolution of average risk level for a specific service (resp. primary asset)

	Evolution of risk level for a specific supporting asset
	Comparative overall risk summary
	Evolution of unacceptable risks ratio
	Evolution of unacceptable risks ratio for a specific service (resp. primary asset)
	Evolution of the overall average risk level of unacceptable risks
	Evolution of the average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	Evolution of Top 10 threats leading to risks with the highest current risk level
	Evolution of Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Evolution of Top 10 vulnerabilities the most exploited
	Evolution of Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Evolution of Top 10 most targeted supporting assets
	Evolution of Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Evolution of Top 10 security measures
Security objectives	Evolution of sophistication levels breakdown
	Evolution of Top 5 Security Objectives with the highest sophistication level
	Evolution of Top 5 Security Objectives with the lowest sophistication level
	Evolution of Security Objectives sophistication level per SO
	Evolution of Security Objectives sophistication level per domain
Maturity / Risk management ratios	Evolution of Maturity / Risk management ratio (physical and environmental security)
	Evolution of Maturity / Risk management ratio (technological security)
	Evolution of Maturity / Risk management ratio (human resources security)
	Evolution of Maturity / Risk management ratio (incident management and contingency plan)
	Evolution of Maturity / Risk management ratio (operational security)

Annex II: Measurement set for the Operator of Essential Service

Measurements to Analyse the OSE security level for a specific year (based on a specific risk assessment report)

General information on risks	Overall average risk level
	Average risk level for a specific service (resp. primary asset)
	Average risk level for a specific supporting asset
	Overall current risk levels distribution
	Current risk levels distribution for a specific service (resp. primary asset)
	Overall estimated residual risk levels distribution
	Estimated residual risk levels distribution for a specific service (resp. primary asset)
	Overall risk summary
	Unacceptable risks ratio
	Unacceptable risks ratio for a specific service (resp. primary asset)
	Overall average risk level of unacceptable risks
	Average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	List of supporting assets associated to a specific service (resp. primary asset)
	List of threats considered for a specific service (resp. primary asset)
	List of vulnerabilities considered for a specific service (resp. primary asset)
	List of controls considered for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest current risk level
	Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Top 10 threats leading to risks with the highest estimated residual risk level
	Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Top 10 vulnerabilities the most exploited
	Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Top 10 most targeted supporting assets
	Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Top 10 security measures
Security objectives	Sophistication levels breakdown
	Security Objectives ranking by sophistication level
	Security Objectives sophistication level per SO
	Security Objectives sophistication level per domain
Maturity / Risk management ratios	Maturity / Risk management ratio (physical and environmental security)
	Maturity / Risk management ratio (technological security)
	Maturity / Risk management ratio (human resources security)
	Maturity / Risk management ratio (Incident management & contingency plan)
	Maturity / Risk management ratio (Operational security)

Measurements to analyse the evolution of the OSE security level (based on numerous risk assessment reports)

General information on risks	Evolution of overall average risk level
	Evolution of average risk level for a specific service (resp. primary asset)
	Evolution of risk level for a specific supporting asset
	Comparative overall risk summary
	Evolution of unacceptable risks ratio
	Evolution of unacceptable risks ratio for a specific service (resp. primary asset)
	Evolution of the overall average risk level of unacceptable risks
	Evolution of the average risk level of unacceptable risks for a specific service (resp. primary asset)
Risk concepts	Evolution of Top 10 threats leading to risks with the highest current risk level
	Evolution of Top 10 threats leading to risks with the highest current risk level for a specific service (resp. primary asset)
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level
	Evolution of Top 10 threats leading to risks with the highest estimated residual risk level for a specific service (resp. primary asset)
	Evolution of Top 10 vulnerabilities the most exploited
	Evolution of Top 10 vulnerabilities the most exploited for a specific service (resp. primary asset)
	Evolution of Top 10 most targeted supporting assets
	Evolution of Top 10 most targeted supporting assets for a specific service (resp. primary asset)
	Evolution of Top 10 security measures
Security objectives	Evolution of sophistication levels breakdown
	Evolution of Security Objectives ranking by sophistication level
	Evolution of Security Objectives sophistication level per SO
	Evolution of Security Objectives sophistication level per domain
Maturity / Risk management ratios	Evolution of Maturity / Risk management ratio (physical and environmental security)
	Evolution of Maturity / Risk management ratio (technological security)
	Evolution of Maturity / Risk management ratio (human resources security)
	Evolution of Maturity / Risk management ratio (incident management and contingency plan)
	Evolution of Maturity / Risk management ratio (operational security)

List of abbreviations

Abbreviation	Translation
API	Application Programming Interface
CERT	Computer Emergency Response Team
CIRCL	Computer Incident Response Center Luxembourg
CSIRT	Computer Security Incident Response Team
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DSP	Digital Service Provider
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
ISAC	Information Sharing and Analysis Center
MISP	Malware Information Sharing Platform
NCA	National Competent Authority
NISDUC	NIS Directive User Community
NOC	Network Operation Centre
OES	Operator of Essential Services
OTRS	Open-source Ticket Request System
PSIRT	Product Security Incident Response Team
RESTful	Representational State Transfer
RIPE	Réseaux IP Européens
RTIR	Request Tracker for Incident Response
SOC	Security Operations Center
SPOC	Single Point of Contact
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated Exchange of Intelligence Information
URL	Uniform Resource Locator

Terms and definitions

Cloud computing service	A digital service that enables access to a scalable and elastic pool of shareable computing resources [1].
Digital Service	Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services [1]. For the scope of the NIS Directive, only three types of services (as defined in Annex III of the Directive) are considered: • Cloud computing service. • Online marketplace. • Online search engines.
Digital Service Provider	An entity that provides digital service(s).
Incident	Any event having an actual adverse effect on the security of network and information systems [1].
National Competent Authority	An authority designated by each Member State in charge of monitoring the application of the NIS Directive at national level [1].
Network and information system	(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, (c) perform automatic processing of digital data; or digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance [1].
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
Online marketplace	A digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace [1].
Online search engine	A digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found [1].
Operator of Essential Services	A public or private entity of a type referred to in Annex II of NIS Directive, which meets the criteria laid down in Article 5(2) of the NIS Directive [1].

Risk	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems [1].
Security of network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems [1].
Single Point of Contact	An entity designated by each Member State in charge of exercising a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group and the CSIRTs network [1].
WHOIS	TCP-based transaction-oriented query/response protocol, widely used to provide information services to Internet users [25].

Bibliography

[1] NIS Directive, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32016L1148

[2] D3.1: NISDUC Lessons learnt – vol.1, available on https://www.nisduc.eu/fileadmin/files/resources/D3.1-NISDUC_Lessons_learnt_vol.1.pdf

[3] ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

[4] MISP Threat Sharing, https://www.misp-project.org/

[5] IntelMQ repository on Github, https://github.com/certtools/intelmq

[6] Call for Tender, Preparatory activities for the launch of the connecting Europe facility (CEF) core cooperation platform for computer emergency and response teams in the European Union — SMART 2014/1079, European Commission, 16 September 2014, https://digital-strategy.ec.europa.eu/en/funding/preparatory-activities-launch-connecting-europe-facility-cef-core-cooperation-platform-computer

[7] Introduction to Structured Threat Information Expression (STIX), OASIS, https://oasis-open.github.io/cti-documentation/stix/intro

[8] Introduction to Trusted Automated Exchange of Intelligence Information (TAXII), OASIS, https://osis-open.github.io/cti-documentation/taxii/intro

[9] Jira Software, Atlassian, https://www.atlassian.com/en/software/jira

[10] Open-source Ticket Request System (OTRS), https://otrs.com/

[11] Best Practical, Request Tracker for Incident Response, https://bestpractical.com/rtir

[12] Ted-eTendering, Call for tenders' details, SMART 2015/1089, Connecting Europe facilities cybersecurity digital service infrastructure, European Union, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=1428

[13] Ted-eTendering, Call for tenders' details, SMART 2018/1024, Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs –MeliCERTes Facility, European Union, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4340

[14] CISRTs Network, https://csirtsnetwork.eu/

[15] Cerebrate Project, the open-source directory and orchestrator for security tools, https://www.cerebrate-project.org/

[16] Call for Tender, A call for tender to support the work of the NIS Cooperation Group, 31 May 2019, European Commission, https://digital-strategy.ec.europa.eu/en/funding/call-tender-support-work-nis-cooperation-group

[17] Activities, The Digital Europe Programme, European Commission, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[18] Product Security Incident Response Teams (PSRIT) Services Framework, FIRST, https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

[19] Data Protection and Privacy Issues, Internet Corporation for Assigned Names and Number (ICANN), https://www.icann.org/dataprotectionprivacy

[20] Directive (EU) 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the

authorisation of electronic communications networks and services, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140

[21] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

[22] Guideline on Security Measures under the EECC, ENISA, December 10, 2020, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

[23] ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management

[24] ISO/IEC 27001:2013 - Information technology - Security techniques -Information security management systems - Requirements

[25] RFC 3912, WHOIS Protocol Specification, https://datatracker.ietf.org/doc/html/rfc3912