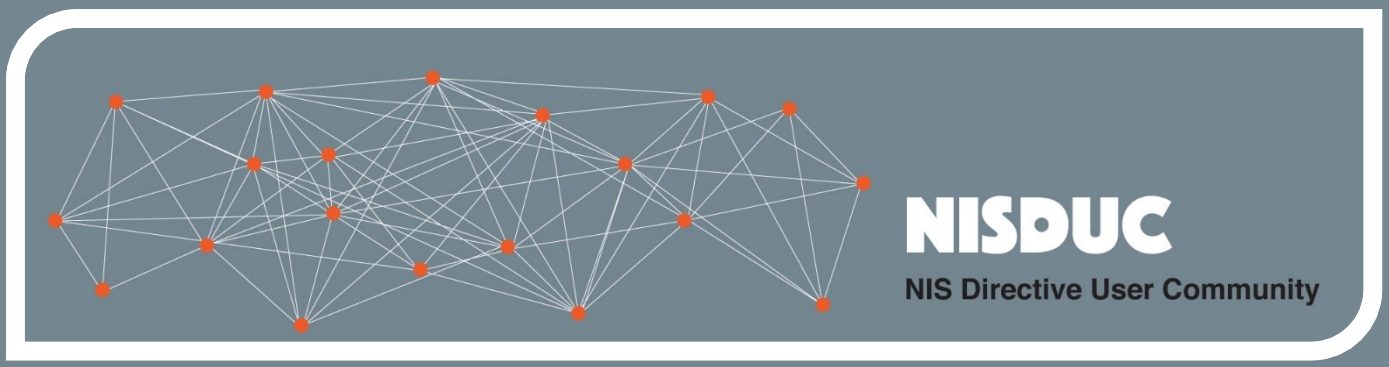

D3.1: NISDUC Lessons learnt – vol.1

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	D3.1 / V1.0
Activity contributing to the deliverable	Activity 3: Monitoring on the practices and experiences of the implementation of the NIS Directive
Due date	30/06/2021
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, Ricardo Lopes, Sheila Becker (**ILR**)

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

Alexandre Dulaunoy, Gérard Wagener (**SECURITYMADEIN.LU**)

Reviewers

Caroline Breure (**CCB**)

Disclaimer

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 studies set up 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.

Sector modelling

In Article 14 of the NIS Directive [1] on security requirements for OES, it is stated that:

> *"1. Member States shall ensure that operators of essential services take **appropriate and proportionate technical and organisational measures to manage the risks** posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those **measures shall ensure a level of security of network and information systems appropriate to the risk posed**.*
>
> *2. Member States shall ensure that operators of essential services **take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems** used for the provision of such essential services, with a view to ensuring the continuity of those services."*

According to the NIS Cooperation Group publication 01/2018 [2], the security measures must be "*effective, tailored, compatible, proportionate, concrete, verifiable and inclusive*". In this sense, the adoption of a risk assessment process to determine risks and the appropriate and proportionate measures is strongly encouraged[1]. Thus, a yearly security risk assessment by OES is considered the most effective way to comply with the NIS Directive. Being part of the security risk management process, the risk assessment includes the establishment of the associated risk treatments. The obtained results will be then reported to the NCA to guarantee an overview of risks and measures. The results will then be analysed by the NCA with respect to state of the art of the risk management approach.

To facilitate the work of OES and harmonize the content, depth and quality of the previously mentioned reports, a strong guidance for reporting is identified as a prerequisite by ILR and BIPT for their respective regulated entities. To facilitate the work of the NCA, it is necessary to adopt a homogeneous, standard, and easy-to-compare and analyse risk assessment process. Such guidance relies on a common methodology and its associated comprehensive software platform SERIMA (see Information systems security section, p.14), on the one hand, and on the definition of sectoral models,

[1] *PART 1 – GOVERNANCE AND ECOSYSTEM – 1.1 Information System Security Governance & Risk Management – Information system security risk analysis*

to allow a pooling of efforts for the identification of OES infrastructure elements, on the other. As shown in Figure 1, the 'Risk Management' module is populated by '*Reference Models*' in order to obtain a 'Measurement' framework to analyse OES and the different sectors supported by an advanced 'Data analytics' module.

Such a common methodology allows the NCA to optimize the essential sectors overview and provides several benefits, such as:

- A risk profile for each OES
- A risk profile for the whole sector
- Benchmarks between two or more distinct OES
- Individual reports

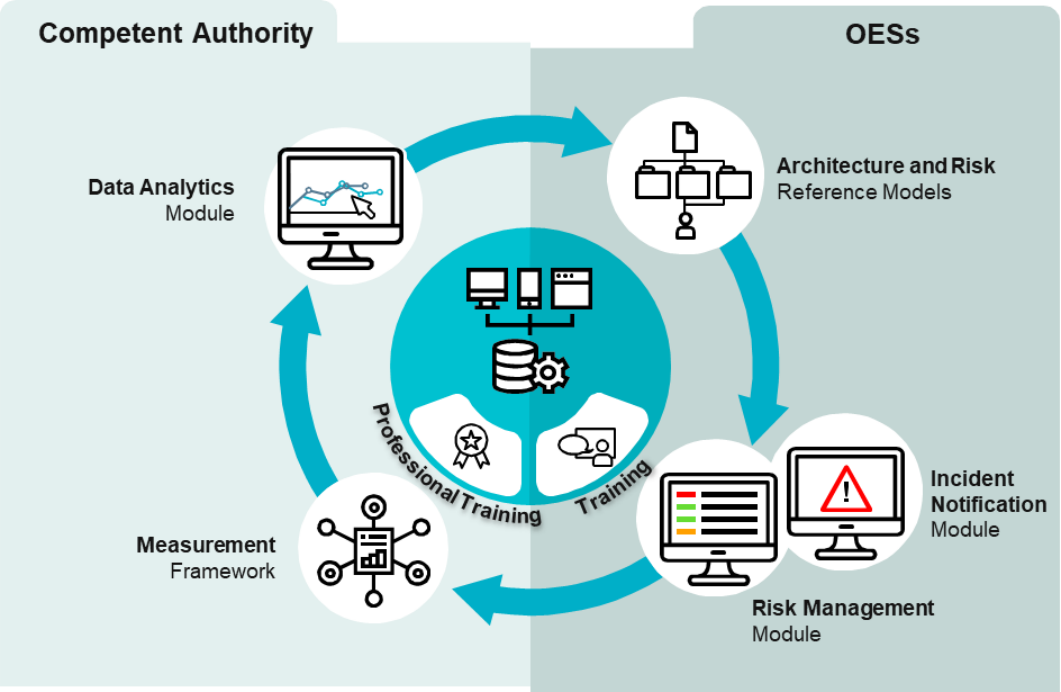

Figure 1: Overview of the SERIMA platform

The modelling effort is undertaken at two levels, as depicted in Figure 2:

- A regulatory model that establishes a common risk management methodology adapted to the NIS Directive and all its associated rules. This model is common to every sector/sub-sector of NIS. Other regulatory models are available, such as one supporting the European Electronic Communications Code Directive [3] and another supporting the ISO/IEC 27001 standard [4].
- Sectoral models composed of libraries specific to one sector/sub-sector. For each sector/sub-sector, sector-specific libraries are provided for primary assets, supporting assets, threats and vulnerabilities.

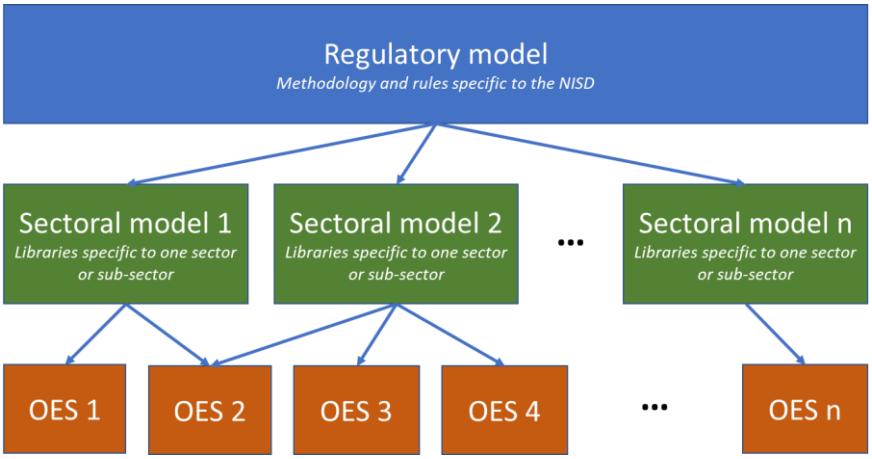

Figure 2: The methodology composed of models on two levels

Both models were designed using a user-centred design approach and cooperative design, meaning that for each sector/sub-sector identified by the NIS Directive, a series of workshops or focus groups took place. The workshops brought together all the OES identified for each sector/sub-sector (represented by the person(s) expected to perform the required security risk management tasks).

During these workshops, the specificities of each sector/sub-sector were collected, including the main activities, a common catalogue of infrastructures (libraries) and main (priority) risks. From the point of view of an OES, the identification of these common characteristics allowed the establishment of sectoral models for the following purposes:

- Defining a common level in terms of the scope of OES risk assessment from a business perspective;
- Accelerating the identification of infrastructure elements;
- Developing a common language for a given sector;
- Structuring and standardizing the risk management approach.

The methodology developed is largely based on the well-known international standard ISO/IEC 27005 [5] on Information security risk management. Concretely, the modelling of each sector/sub-sector follows a dedicated methodology, as described below and illustrated in Figure 3.

Step 1: Modelling of the primary assets based on the essential services and sub-services (business activities)

The first step consists of defining the different activities that make up each essential service. A literature review is performed in order to identify relevant documents for the sector/sub-sector addressed. Then, based on this literature review, a first workshop is organized with all the OES of that sector/sub-sector, and a set of common activities, such as business sub-services and capabilities (how the service is delivered), is established and associated with each essential service.

Step 2: Modelling of the supporting assets of the essential services through an information system architecture

The second step consists of describing the information system supporting each essential service; this is common to all the OES of the working group. Listing the components that implement each service allows the relevant threats and vulnerabilities to be identified and traces these back to the actual service. The main challenge in this activity is to select the right level of abstraction in the description of the information system, while taking into account the following objectives:

- describing the information system for the main purpose of security risk management,
- producing models applicable to all operators providing the essential service. The information system is then described following the ISO/IEC 42010 standard [6].

Step 3: Definition of the service-related knowledge base of risks

The objective of this third step consists of:

- the identification of the most relevant threats and vulnerabilities for each essential service;
- the definition of the impact scales specific to the sector/sub-sector.

A generic knowledge base is established for threats and vulnerabilities and is made available to help OES to select their relevant risks. In addition, each sector/sub-sector identifies its own '*mandatory*' threats to be considered. This service-related minimum risk knowledge base, specifically designed for the OES of a sector/sub-sector, is not intended to replace the risk identification made by each individual OES, but to provide better guidance during this step and clearly delimit the scope of the analysis. Indeed, a key issue in risk management is the risk identification activity, which roughly consists of defining the relevant risks, and thus the relevant threats, vulnerabilities and impacts regarding the business operated and the architecture in place. Some generic knowledge bases already exist, helping the analyst in the risk identification phase. However, for those without experience, it is generally difficult to operate such a knowledge base and determine the relevant sets of risk they need to consider. Thus, a set of '*mandatory*' threats is selected by the working group to have a first basis of work. In addition, the impact scales are fine-tuned in order to integrate their particularities and the sector '*language*'. In the framework of their information security risk management process, for a given service, OES will have to indicate whether (pre-selected) threats apply, and how their system is vulnerable. It will, however, also remain important for each OES to think about their specificities (at the business or architecture level) potentially implying specific risks, involving non pre-selected threats and/or vulnerabilities.

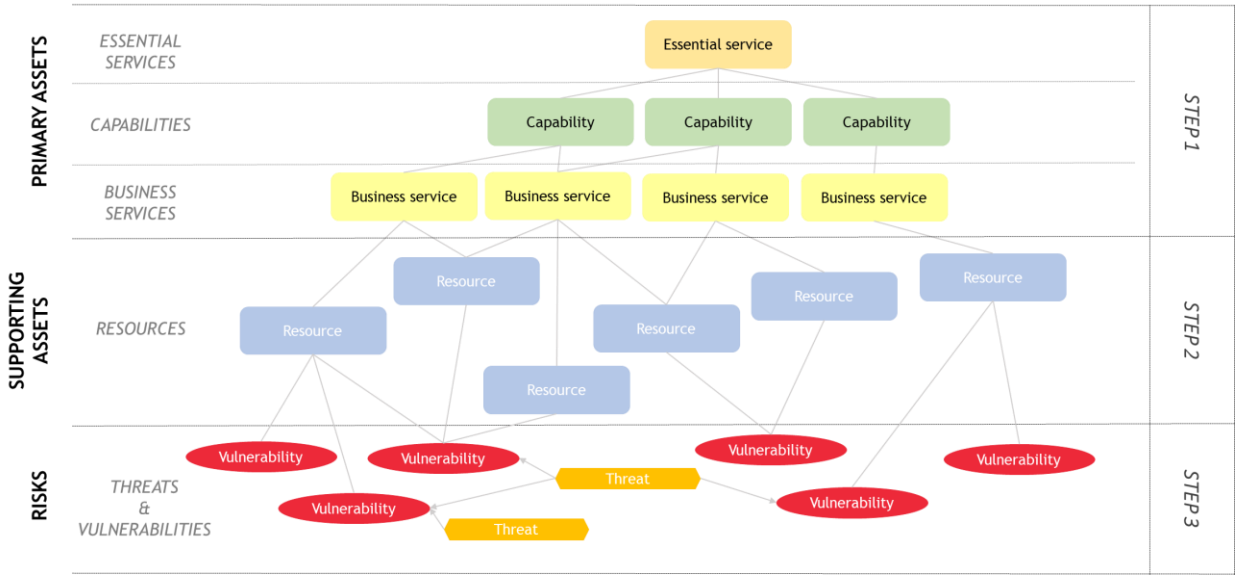

Figure 3: Sectoral modelling methodology and correspondence between architectural elements and elements of the risk assessment

The various artefacts produced within the framework of this approach are subsequently transformed into libraries used by a dedicated risk management tool (cf. section Sector-specific risk assessment approach, p.14).

Methodology application feedback

This methodology was used in Luxembourg by LIST and ILR for several months in 2020 and 2021, to develop models of the following NIS sectors/sub-sectors:

- Energy/Electricity
- Energy/Gas
- Transport/Air transport
- Transport/Rail transport
- Transport/Road transport
- Health sector
- Drinking water supply and distribution
- Digital Infrastructure/DNS service providers
- Digital Infrastructure/TLD name registries

For each of the sectors/sub-sectors, a series of workshop consisted of a minimum of four workshops organized as follows:

- **WS 1:** Global presentation, identification of primary assets by defining the sub-services (step 1).
- **WS 2:** Identification of supporting assets and their mapping with sub-services (step 2).
- **WS 3:** Identification of risks with the selection of the most relevant threats (step 3).
- **WS 4:** Identification of risk assessment methodology specificities by defining the impact criteria (step 3).

Internally at LIST, a reference model entitled R-EAM4REG (*Reference Enterprise Architecture MetaModel for Regulation*) was used to model the sector/sub-sector, with a focus on architecture. This metamodel was useful as a support for establishing the expected architecture, and clarifying the identification of all the expected elements, the different layers, and interactions between them. Part of this metamodel is presented in Figure 4. This metamodel was useful for building each sectoral model in Figure 3 in more detail. However, the model was only used for scientific purposes and was never shared with the working group so as not to confuse them and remain at a pragmatic level as in Figure 3.

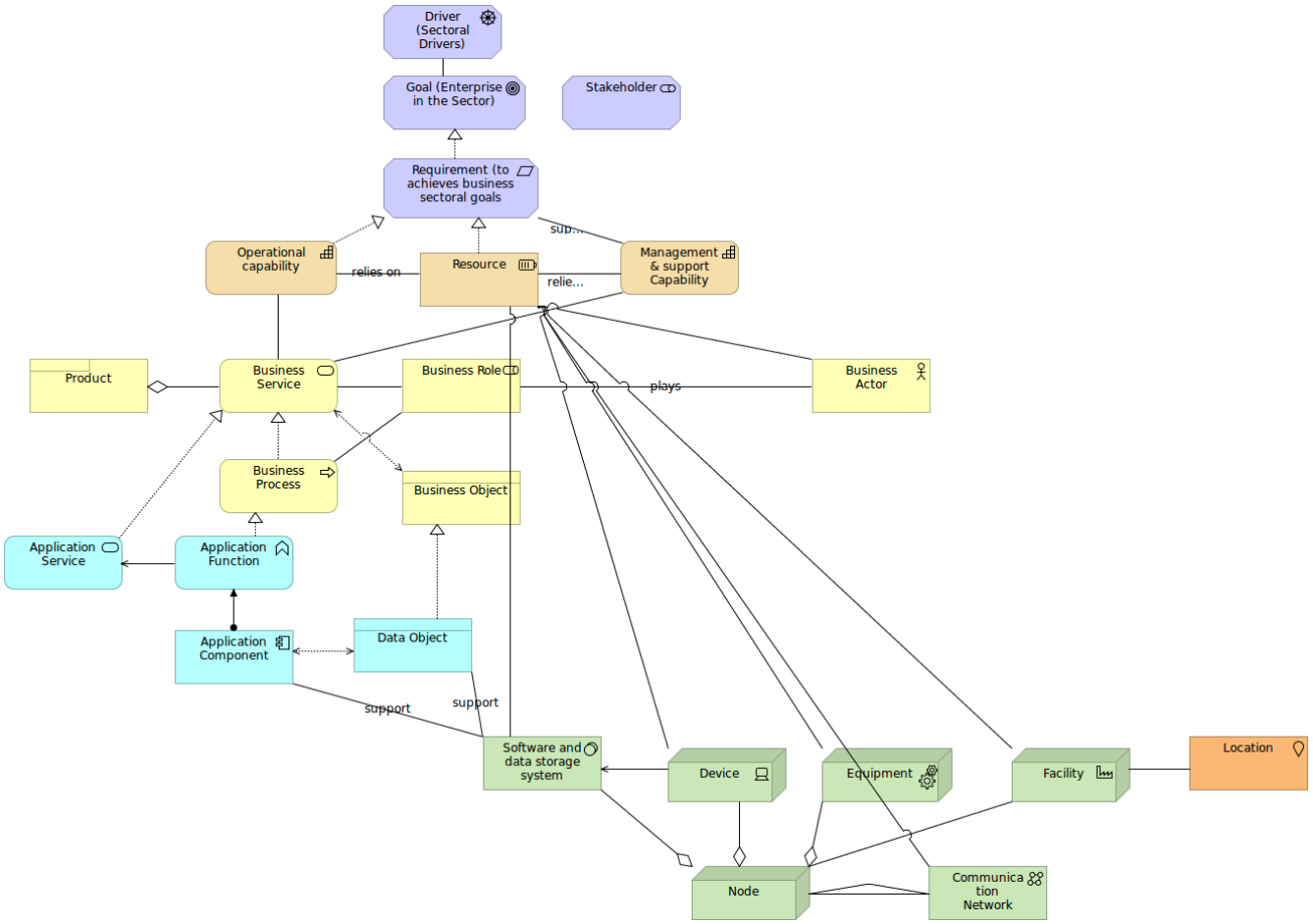

Figure 4: Reference model to be instantiated

At the end of each series of workshops, the following results were compiled for each sector/sub-sector in a sectoral model composed of the following libraries:

- Primary assets, expressed as essential services composed of one or several sub-services;
- Supporting assets, with their mapping to sub-services (primary assets);
- Threats, with a first selection of some threats for which assessment is considered mandatory in order to guarantee the quality of the results;
- Vulnerabilities, with the most relevant vulnerabilities for each threat in each sector/sub-sector;
- Dedicated impact criteria usually expressed as the number of users affected and expected unavailability.

The first step in defining the primary assets was the easiest. Indeed, the activities of the OES in one sector or sub-sector in Luxembourg are usually similar or even standardized. Moreover, only common sub-services were identified, as the OES are free to add specific sub-services individually later. A description of each sub-service was added to allow a better understanding and each OES may make the link with its own business activity.

The next step consisted of listing all relevant supporting assets used in each sub-service. The supporting assets in the frame of the NIS Directive are all elements used by the following types of information system:

- Hardware
- Software
- Network
- Site
- Personnel
- System
- Outsourced service

It should be noted that for this exercise, only specific elements of the sector/sub-sector in question had to be added. Indeed, to facilitate and standardize the work of the OES, all supporting assets generic enough to be useful in any sector/sub-sector, were identified beforehand and grouped into a so-called *IT-Generic* list. This generic IT list, presented in the following table, was very useful during the workshops, especially to save time.

NAME	TYPE	NAME	TYPE
Fileserver	Hardware	**Wireless network**	Network
Firewall	Hardware	**Decision maker**	Personnel
Fixed voice device	Hardware	**Developers**	Personnel
Laptop computer	Hardware	**IT Operation/Maintenance staff**	Personnel
Load balancer	Hardware	**Users**	Personnel
Mail server	Hardware	**Air conditioning**	Site
Printer	Hardware	**Datacenter**	Site
Proxy server	Hardware	**External environment**	Site
Removable media	Hardware	**Server room**	Site
Router	Hardware	**Power supply**	Outsourced service
Server	Hardware	**Telecommunications services**	Outsourced service
Smartphone	Hardware	**Water supply**	Outsourced service
Storage	Hardware	**CRM - Customer Relationship Management**	Software
Switch	Hardware	**DBMS - Database Management System**	Software
Workstation	Hardware	**Electronic messaging software**	Software
Ethernet network	Network	**ERP - Enterprise Resources Planning**	Software
Internet	Network	**IT Monitoring system**	Software
Intranet	Network	**Operating system**	Software

The mapping between all supporting assets and sub-services was more challenging since technical assets are not used by all OES in a standardized way. To reach a consensus within a sector/sub-sector, a voting system was set up to establish this mapping and obtain a pre-selection of supporting assets for each sub-service. However, each OES is free to add, remove or modify any supporting assets to answer to its specific needs.

Regarding the library of threats, a list of 42 threats was defined before the workshops based on the international standard ISO/IEC 27005 [5]. From this list, some were selected by the OES of one sector/sub-sector (via a voting system) that were obvious and important to consider, and these threats then became mandatory for each sub-service and were pre-selected in the tool. However, as is usual, each OES was totally free (and indeed, was encouraged) to select more threats specific to its activity or specific to one sub-service.

The final step during workshops was to establish the impact criteria specific to the sector/sub-sector. To eliminate the maximum subjectivity in the impact scale, we proposed a two-dimensional approach and thus, we defined two sub-scales. These two sub-scales are usually expressed in number of users affected and expected unavailability (both to reflect the NIS Directive view and based on our previous

successful approach with the Telecommunications sector [7]). Finally, the two sub-scales were automatically combined, and the risk impact was expressed with a ranking of: *Low* / *Medium* / *High* / *Very high*. Figure 5 shows a fictitious example of two sub-impact scales with the final impact scale combining the two sub-scales. In each working group, we established the correct definitions of the 5 levels of the two sub-scales together, in order to be coherent with the sector/sub-sector, measurable, and have the specific vocabulary. If required by a sector/sub-sector, the title of the sub-scales may be modified, especially if the number of users is not directly measurable, in order that better parameters can be chosen, such as the number of trains affected (passenger or freight).

This step was very important for defining impacts with the sector/sub-sector and establishing scales for things that are measurable and relevant to them. This step was also very important for adapting the methodology to one specific challenge of the NIS Directive: that risk management is not (as is usually the case) based on the organization's view but is focused on the citizens that use the service. Consequently, the impact scale should reflect this: a risk with a '*high*' impact on the organization is not necessary a risk with a '*high*' impact in the scope of the NIS Directive and vice versa.

	Users affected (nationally)
1 - Very low	More than 50 users
2 - Low	More than 1% AND more than 500 users
3 - Medium	More than 5% AND more than 5000 users
4 - High	More than 10% AND more than 15.000 users
5 – Very high	More than 25% AND more than 50.000 users

	Expected unavailability
1	Less than 4 hours
2	Between 4 hours and 24 hours
3	Between 1 day and 2 days
4	Between 2 days and 4 days
5	More than 4 days

		Users affected (nationally)				
		1	2	3	4	5
Expected unavailability	1	Low	Low	Low	Medium	High
	2	Low	Low	Medium	Medium	High
	3	Low	Medium	Medium	High	High
	4	Medium	Medium	High	High	Very high
	5	Medium	High	High	Very high	Very high

Figure 5: Fictitious example of impact scales

The collaborative approach with these workshops involving OES was very useful. Indeed, the objective of facilitating the work of OES was achieved with the establishment of tailored models specific to different sectors/sub-sectors. In addition, these workshops enabled privileged communication with OES on many points:

- Explaining details of the NIS Directive;
- Explaining the requirements of the NIS Directive and how to comply with it;
- Specifying the scope;
- Involving and empowering OES;
- Explaining our risk assessment methodology to OES and training them in it;
- Understanding the particularities of each sector/sub-sector;
- Collecting OES' expectations;
- Gathering OES' needs in terms of tools;
- Answering questions.

One of the major challenges in this collaborative approach was finding the right level of sectoral models. If the sectoral model is too high-level, then it is standardized and useful for NCA, but less usable and useful for OES. On the other hand, if the sectoral model is too specific and pragmatic, then it saves a lot of time for OES, but the model approach loses its interest. This 'right' level of abstraction for sectoral models differed between sectors/sub-sectors, depending mainly on the number of OES in the sector/sub-sector and the level of standardization of the activities of the sector/sub-sector.

Finally, despite the somewhat "unusual" nature of this collaborative approach, bringing together different OSE, who for some of them are competitors, this approach was well received and well accepted by OES. This brought motivation, good participation, and therefore relevant results.

Information systems security

The objective of the NIS Directive is to achieve a high common level of security of network and information systems across the European Union by establishing, among others, security measures for Operators of Essential Services.

Article 14 of the NIS Directive defines the security requirements of OES as being to "*take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations*."

This chapter identifies a general approach for NCAs to help OES meet the obligations set out in the NIS Directive based on experience gained in Belgium and Luxembourg in relation to the NIS Directive but also based on experience that had already been gained in the Telecommunications sector over several years.

In order to identify appropriate and proportionate measures with respect to potential risks, a risk assessment is the most adequate approach. Therefore, the OES need to provide the results of their risk assessments to the respective competent authorities at least once per year. Additionally, it is also considered useful for OES to submit an updated risk assessment to the NCA when important structural or technical changes have been made to or in the organization.

The objective of the yearly submission of the risk assessments is twofold. Firstly, it is considered a major part of securing the systems essential to our society and economy. Secondly, it is considered a part of the awareness-raising of the risks, threats and impacts in the field of cybersecurity.

To establish and update a risk assessment, OES need to evaluate the areas of IT or networks that are essential for delivering their services to customers. Assets need to be defined, threats considered, and decisions made in order to mitigate risks. This work will of course lead to the OES having an overview of their infrastructure and services. As well as being better prepared against cyberthreats, OES also gain awareness of existing threats and vulnerabilities.

In the following section, a more detailed view of a sector-specific risk assessment will be given.

Sector-specific risk assessment approach

Many different methodologies for risk assessment exist, however, they all have one thing in common. They are usually high-level frameworks that the risk manager completes with more specific information. These methodologies provide valuable information on how to carry out a risk analysis and what procedures should be prepared. However, they are very generic, and are neither technical nor sector-specific.

As the essential sectors become more and more digitalized, it is crucial to be able to take an in-depth look at the risks of the different sector-specific equipment and assets. In this sense, the idea of a sector-specific approach is to gain knowledge of the different more technical assets, which are essential for providing services.

Considering that the expert knowledge lies with the OES, several workshops were held for the NCA to identify the sector-specific assets together with the OES. These workshops were organized per sector, so that the identified assets were also sector-specific. This means that a common baseline was created for each sector concerning the different areas of risk management (primary assets, secondary assets, threats, vulnerabilities, risks) in collaboration with the OES of the different sectors during 3-5 workshops per sector. This common baseline was then organized into one library per sector (see Sector modelling section, p.6), which was subsequently made available for the whole sector on a risk assessment platform [8].

In order to facilitate risk assessment for the OES, a platform was made available to all OES. The added value of this platform is the sector-specific approach, meaning that different sectors have a different defined baseline (primary assets, supporting assets, etc) due to the sector-specific workshops described above. Due to the common baseline, the OES have access to a sector-defined model to evaluate their own risk assessment.

In addition to the risk assessment, more generic questions are posed in the submission process concerning the organization of the operator and the security objectives. These questions are based on the security objectives established by ENISA for the Telecommunications sector [9]. Due to the general nature of these questions, these security objectives are easily adaptable for the NIS sectors. They also give a good overview on the maturity of the different measures taken by the OES.

Annual regulatory reports

As already mentioned, the OES are required to submit their risk assessment to the NCA on a yearly basis. In the event that the OES use the platform, the NCA can make an anonymized comparison within the sector and maybe to some extent with other sectors. This anonymized comparison is presented to the OES on a yearly basis, to show the development of the different risks in the sector and the different approaches to address them.

Subsequently, the OES receive personalized reports on their assessment with a comparison to the sector average for risk assessments. This feedback will sensitize the OES to their own risk assessment and indicate what they need to adapt in the future and where they potentially have to improve to be well-prepared for cyber incidents or attacks.

Future steps and challenges

The approach presented above is a crucial step in the right direction, however, there are still some challenges to be faced. It is of fundamental importance to create incentives for OES to use the risk assessment platform to submit their risk assessments. This is important in order to be able to make better comparisons, since having more OES and more risk assessments will result in more adequate sectorial overviews of the sector-specific risks and threats. This will enable both the NCA and the OES to gain more factual information about the whole sector. In return, it will also allow the OES to obtain better and more specific feedback concerning individual risk assessments. This is an important part of protecting against cyber-attacks on essential services in the future.

The current regulation does not foresee a specific bi-directional communication with the OES. Apart from the annual individual report to the OES, defining more feedback to the OES would not only create

incentives to use the risk assessment platform, but would also be beneficial to the overall security and risk assessments of all the essential sectors. In this sense, it is planned to integrate information from the incident notification module of the OES to the risk assessment module of the OES. Additionally, the incident information received from the incident notification module can help the whole sector, by making pertinent information immediately available to the whole sector in an anonymized way.

Besides setting incentives, it is also essential to prescribe what an OES has to submit as a risk assessment when not using the platform. This is crucial because the more the information submitted outside the platform is similarly structured, the easier it will be to include those risk assessments in the sectorial comparisons. Subsequently, this will help give better feedback to the OES and further improve the risk assessments and enhance the preparedness for cyber-incidents that the essential services will face.

One major current issue with risk assessment is that the risks are evaluated based on subjective information. If the OES had a broader range of information available for their risk assessment, the evaluation would be more objective and coherent with the rest of the sector and the evaluation would be more factual.

Therefore, it is crucial to promote information exchange and to be able to give guidance and best practices to OES. NCA should work on giving increased guidance, so that the whole sector has a common understanding of current threat scenarios and impacts of specific vulnerabilities.

However, this guidance can only be given when the NCA has enough information available to create guidance. That guidance can also be based on anonymized information on threats and incidents. If the OES see a benefit in sharing more information, then they will also be willing to share more information, not only with the NCA but also and especially with the sector. The usage and adoption of the MISP (Malware Information Sharing Platform) [10] is a perfect example of the interplay between sharing information and gaining knowledge from the information shared by others.

Creating and providing this factual information is crucial for OES to make informed decisions on sector-specific risks and threats. The formulation of this guidance will be the main focus of the NCA in the future and the more the sectors collaborate, the better the guidance will be. This formulation is not necessarily done at the national level, since the information would be even more pertinent when other countries and OES contribute. The ultimate goal is to create a Europe-wide guidance for all sectors.

Incident notification

The NIS Directive covers a large number of sectors. These sectors are made of entities that may have very different characteristics, particularly in terms of size or activity. These entities may also be subject to various legal obligations, in particular, relating to security, data protection, privacy or economic regulation.

Like other countries, Belgium has transposed the NIS Directive into Belgian law by assigning the supervision of the NIS Act to the sectoral authorities, which are distinct from the national SPOC (Centre for Cyber security Belgium, CCB), the national CSIRT (Centre for Cyber security Belgium, CCB) or the national crisis centre.

Initial discussions on the implementation of the NIS Directive highlighted the importance of facilitating exchanges between the various authorities concerned and the operators of essential services as much as possible.

This is even more relevant for incident notification obligations and the management of such incidents. The various incident response activities must indeed be coordinated immediately, effectively and efficiently. These activities include, for instance, measures to limit, reduce or stop the impact on the service, or measures to manage the impact on service provision.

A practical solution was sought to respect the following points:

- the notification takes place as quickly as possible to minimize the burden for the notifier;
- the content of the notification is delivered immediately to the competent authorities;
- not all elements of a notification are known when an incident is identified;
- the notification is not a substitute for incident management but can be used to request support;
- means of notification already exist in different sectors.

These points have resulted in the authorities building a common notification platform.

The first step was the definition of a common notification form for the various sectors that respected the obligations enshrined in the NIS Directive and the needs of the national authorities.

The second step was the creation of a web platform on which to complete the form.

It was decided that the notifying body should work in three steps:

- A first notification should be issued without delay, even if not all relevant information is currently available. The purpose of this first notification is to draw the attention of the competent authorities to the incident and its possible consequences.
- Additional notifications can be sent periodically as soon as new information becomes available. The purpose of these additional notifications is to update the competent authorities on the status of the incident.
- A potential final report (at the request of one of the above-mentioned authorities) containing all information is sent to the competent authorities. The purpose of this final report is to give an overview of the incident and enable conclusions to be drawn from it.

The notification form includes all available information allowing the nature, causes, effects and consequences of the incident to be determined. Nevertheless, not all fields are required to be filled in for the first notification.

In practice, the notifications must be sent to several authorities. This is done in a single step via the NIS notification platform [11]. It should be noted that telecommunications operators use the same platform and the same information exchange mechanisms.

The form gives the possibility of introducing references to other ticketing systems. This feature is important for keeping the links between the platforms used by the various players.

The information provided to the authorities may be exchanged with the authorities of other EU member states and with other Belgian authorities where this is necessary for the enforcement of legal provisions.

However, such a transmission of information is limited to what is relevant and proportionate to the purpose of such an exchange, in compliance with the GDPR Regulation [12], the confidentiality of the information concerned, and the security and the business interests of the notifier.

The obligation to notify possible personal data breaches to one of the national competent data protection authorities via the appropriate notification tools is also stated via a warning on the form

and a link to the website of the Data Protection Authority as a reminder to entities that are subject to the NIS Directive.

This solution made it possible to efficiently respond to the various constraints. We believe that it is important to be able to link incident notifications to risk analyses and audits in the future. This work will be planned in the coming months.

In Luxembourg, the NIS Directive is transposed in such a way that the ILR is not only the single point of contact but also the competent authority for all sectors (except the financial sectors). However, a similar approach is currently being planned for a single point of entry for the notification of incidents, although not within different NIS sectors (since this is already the case due to the transposition) but with other national authorities that have similar obligations towards the same sectors (i.e. critical infrastructures, and transport). A methodology for this specific Luxembourgish case still needs to be developed and adopted.

Lessons learnt from Computer Security Incident Response Teams (CSIRTs)

In this section, best practices are proposed from the perspective of the Computer Incident Response Center Luxembourg (CIRCL), the CSIRT for the private sector, communes, and non-governmental entities in Luxembourg. Referring to Art. 9 (1) of the NIS Directive [1], a Member State designates one or more CSIRTs to comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, and responsible for risk and incident handling in accordance with a well-defined process. For the local NIS Directive implementation in Luxembourg, two CSIRTs were referenced: GOVCert and CIRCL, with GovCERT focusing on governmental entities and CIRCL on the private ones.

Collaborative incident response

Although only two CSIRTs are mentioned in the national NIS Directive implementation, the local CSIRT capacity is reinforced by private CSIRTs. These private CSIRTs are grouped within a virtual federated environment called CERT.LU. Each member of CERT.LU contributes in some capacity. For instance, CIRCL provides an operational real-time chat infrastructure to which the CERT operators of the different teams have access. This chat is mainly used to coordinate distributed incident responses between multiple teams. Furthermore, regular workshops are organized on CERT.LU where CERT operators can discuss various aspects, such as experiences with tools. Other areas of cooperation are storage capacities, networks and processing, allowing the various teams to share evidences quickly. The real-time communication within this virtual organization helps to speed up the impact assessment of incidents processed in an informal way.

Automation driven data sharing

Threat actors rarely target individual companies, preferring to operate in campaigns aiming to maximize their benefits and targeting multiple companies within a short time frame. Different incident response teams work in parallel on different cases where threat actors use the same attacking techniques. Hence, they are in an arms race with the threat actors and there is a need for efficient automated information sharing.

Sharing of data feeds

Data feeds provide valuable feedback on the security and health of the constituency. They enable to see from an external point of view if systems of the constituents are compromised or if security measures are well applied. Data feeds come from multiple sources such as sinkholing activities, blackhole networks, honeypots. Data feeds from sinkholing activities make it possible to identify compromised systems connecting to the command and control centres. Data feeds from blackhole, honeypot networks allow the identification of scanning activities such as people probing systems for identifying potential vulnerable systems to compromise. They also permit to identify misconfigured systems. Ongoing denial of service attacks can be observed in data feeds from blackhole networks [13]. Honeypot systems provide data feeds about automated attacks.

BGP ranking [14] is an operational platform hosted at CIRCL and was created in 2010 that aggregates numerous data-feeds to rank different internet service providers by their autonomous system numbers. The various patterns of temporal ranks give hints on how abuses are handled by these

network operators, for example, whether they simply ignore all abuse complaints and do bulletproof hosting or whether they take down and clean up systems that behave maliciously. Besides national and governmental CSIRTs, other private entities like *Shadowserver* scan the whole internet multiple times a day, do sinkhole operations and provide the CSIRTs with data feeds of compromised systems. In order to setup and exploit these data feeds, IOC are needed. In this sense, and to share efficiently IOCs among CSIRTs and the private sector, CIRCL operates the threat-sharing platform MISPPRIV [15] where 1741 organizations are registered (as of 2 April 2020).

Hence, if one organization is attacked and shares the IOCs immediately on the platform, then 1740 other organizations can use this information to protect their infrastructure. The platform also has 15,922,870 attributes (containing IOCs), however, a manual notification of IOC is not possible for such a high number. **Hence, automation is the key to allowing the information produced to be used immediately.**

Sharing of observed attacking techniques

Besides the sharing of technical Indicators of Compromise, it is sometimes useful to share the attacking techniques used by the attackers and the nature of the threat actors in order to make strategic decisions to protect an infrastructure. A commonly used framework driven by MITRE is the *ATT&CK framework*, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations [16]. This framework is implemented on the MISP threat-sharing platform [10] but the platform itself is open to other frameworks. The ATT&CK framework is commonly used, mainly by threat analysts, in the MISP community *misppriv.circl.lu* [15]. Information on threat actors that target infrastructures help security analysts to assess the observed attacks. For instance, some threat actors are well known for making targeted attacks and have more focus on an infrastructure than opportunistic attackers. In CSIRT communities, MISP galaxies are used for sharing this kind of information, especially threat actor information [17]. MISP galaxies are maintained by an open-source community; as of 2 April 2021, there are 55 galaxies to describe additional meta information. In the NIS context, the ***cert-eu-govsector*** and ***sector.json*** galaxies might be interesting to model the activity sector. Each sector has a unique identifier to ensure that there are no interpretation errors where an MISP event transits through multiple MISP instances.

Efficient NIS reporting

The NIS Directive provides the legal ground to improve operational cooperation between Member States in managing cyber security incidents. The aim of CIRCL is to support the different actors and thus facilitate collaboration and strategic sharing of cybersecurity information. One key element is the current implementation and deployment of MeliCERTes [18] by the European Commission to improve cooperation and information-sharing platform. MISP is one of the key CSIRT tools for actively using information in MeliCERTes. The aim is to improve the sharing aspect (such as the privacy-aware functionalities), which can help the OES more efficiently share and reuse information from CSIRTs and **improve their notification duties within the NIS Directive.**

As the lead developer of MISP, CIRCL is keen to improve the existing confidence in sharing, as already documented in [19] in order to improve the key activities that stakeholders need to perform within the NIS Directive.

Automating NIS reporting

OES and DSPs already efficiently share Indicators of Compromise, attacking techniques, and additional information required by regulators that is regrouped as MISP galaxies, such as mitre-attack patterns between each other. However, copying and pasting this kind of information into forms for regulators is time consuming for both sides. The regulated entity has to fill in the form and the regulator has to extract the information from the form. Hence, CIRCL made regulator forms available in MISP. A practical example is the *ilr-notification-incident object* [20], which is available in default MISP installations. As each regulator is free to choose its own forms with the pieces of information required, they have the possibility to contribute to the public and open source MISP objects available via pull requests. These pull requests are then reviewed by the maintainers of *misp-objects* and if all tests are passed, they are integrated into the main repository. The names of contributors to MISP objects are publicly available [21]. Automated or semi-automated filling can be implemented with external tools customized to each constituency. If a tool is generic enough to be used by other organizations of the constituency, it is encouraged to be published as open source. Once it is publicly available, it can be referenced on the page dedicated to tools on the MISP website [22].

The concept of informed governance [23] was drawn up and used by the Ministry of the Economy in Luxembourg and used in the context of the national cyber security strategy. The basic principles of informed governance are the consideration of interdependencies between systems, and reliable, comparable and repeatable risk management decisions based on factual information. Software components, like MISP, AIL, D4, BGPRanking, are competent in serving factual reliable data. The ability to structure threat intelligence and NIS reporting information with traceable references helps us get a step closer to repeatable and comparable management decisions. As MISP is a purely decentralized system, traceable references are created with the universal unique identifiers attached to the piece of information that is shared from one organization to another. Each organization also has universal unique identifiers. A decentralized repository of organizations is currently being developed in the project SMART 2018/1024 Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs – MeliCERTes Facility [24]. A practical open source implementation is publicly available on [25]. Such a software could be used to verify the authenticity and contact details of regulators or OES and DSPs.

List of abbreviations

Abbreviation	Translation
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DSP	Digital Service Provider
EECC	European Electronic Communications Code
GDPR	General Data Protection Regulation
IOC	Indicator of Compromise
IT	Information Technology
NCA	National Competent Authority
NISDUC	NIS Directive User Community
OES	Operator of Essential Services
SPOC	Single Point of Contact

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].

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] Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, NIS Cooperation Group, February 2018, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[3] 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

[4] ISO/IEC 27001:2013 – Information technology — Security techniques —Information security management systems — Requirements

[5] ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management

[6] ISO/IEC/IEEE 42010:2011 – Systems and software engineering – Architecture description

[7] Mayer, Nicolas, and Jocelyn Aubert. "*A risk management framework for security and integrity of networks and services*." Journal of Risk Research (2020): 1-12.

[8] Communiqué de presse du 31 Juillet 2020, « *L'ILR lance une nouvelle plateforme d'analyse de risques pour les opérateurs de télécommunications* », Institut Luxembourgeois de Régulation, July, 31st 2020, https://assets.ilr.lu/Documents/ILRLU-1797567310-239.pdf.

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

[10] MISP – Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing, https://www.misp-project.org/

[11] Belgium Incidents Notification Platform, Unified Notification Platform, https://nis-incident.be/en/

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[13] D4 Project website, https://d4-project.org/

[14] BGP Ranking, https://bgpranking.circl.lu/

[15] MISP platform operated by CIRCL, https://misppriv.circl.lu/

[16] MITRE ATT&CK knowledge base, https://attack.mitre.org/

[17] MISP Galaxy repository on GitHub, https://github.com/MISP/misp-galaxy

[18] European Commission, Memo: Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity, http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm

[19] MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, How MISP enables stakeholders identified by the NISD to perform key activities, https://www.misp-project.org/compliance/NISD/

[20] MISP ilr-notification-incident object on GitHub, https://github.com/MISP/misp-objects/blob/main/objects/ilr-notification-incident/definition.json

[21] MISP objects contributors page on GitHub, https://github.com/MISP/misp-objects/graphs/contributors
[22] MISP website, Software and Tools page, https://www.misp-project.org/tools/
[23] François Thill, "Informed governance", in proceedings CLUSIL event, 17 January 2019, Luxembourg, 2019.
[24] Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs – MeliCERTes Facility (SMART 2018/1024) call for tenders' details, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4340
[25] Cerebrate project on GitHub, https://github.com/cerebrate-project