Resilient e-Communications Networks

December 09

Good Practices on Reporting Security Incidents

enisa
European Network and Information Security Agency

Acknowledgements

About ENISA

This report is part of ENISA's Multi-annual Thematic Program One (MTP 1), Resilience of Public e-Communication Networks.

With this Program ENISA, among others, takes stock of and analyses Member States (MS) regulatory and policy environments related to resilience of public e-Communication Networks.

This report is based on the responses given by experts from public and private stakeholders from several Member States and overseas. ENISA would like to thank them all for their excellent contributions and insights.
ENISA would like to thank IDC CEMA for their professionalism and dedication to manage the stock taking and contribute to this report.

Contact details

More information on this report or ENISA's activities on the resilience of public eCommunications Networks can be obtained by

Dr. Vangelis Ouzounis
Senior Expert,
Network Security Policies
ENISA
Email: resilience@enisa.europa.eu, Web: http://www.enisa.europa.eu/act/res

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.
Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.
This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Table of Contents

Executive Summary

The European Commission and Member States pay increasing attention to the resilience of public electronic communications networks. Their aim is to ensure that this infrastructure fulfils its role as a fundamental platform for European societies, economies and institutions.

Incident reporting plays an important role in these efforts as it contributes in improving stakeholders' knowledge of the actual security problems at stake. An effective incident reporting system contributes to the collection of reliable and up-to-date data on information security incidents and ensures: a) quick dissemination of information among interested parties, b) a coordinated response, c) access to a wide pool of expertise about such incidents, d) that national authorities can follow up with the infrastructure managers in a regulatory capacity, e) threat analysis; and f) identification of good practices.

The European Commission has highlighted, in a number of key policy documents, the importance of getting reliable, up-to-date and comparable data on security incidents in order to develop a clear understanding of the nature and extent of the challenges at stake. Such understanding is needed for effective business decision and policy making. The recently adopted reform of the Telecommunications Regulatory Package (article 1313a.3 of the amended Directive 2002/21/EC - referred to as the Framework Directive) specifies that Member States shall ensure that telecom operators 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 their networks. The amended directive further mentions that “The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonizing this provision.”

Recognizing the importance of the topic of incident reporting and the need to prepare the ground for these policy and regulatory developments, ENISA performed an extensive stock taking of Member States activities with the aim to identify and analyse existing practices for incident reporting procedures. The main objective was to identify good practices and to share them with Member States throughout the EU. Such a stock taking of good practices could serve as a basis to the overall discussion on how Member States could best implement the provision on breach notification of article 13 of the revised Framework Directive.

One of the key findings of the stock taking is that the usage of incident reporting schemes across the EU varies widely. Some Member States have very extensive systems, while others have yet to launch one. And even those that do exist vary greatly in their objectives, procedures, types of incidents addressed, participants, and results.

This document examines these practices by first giving a more detailed introduction to the subject of incident reporting and then reviewing the lifecycle of an incident reporting scheme. Based on our analysis we consider the lifecycle as a maturation process that involves the following phases:

- **Identifying the Need.** Before planning a new scheme, it is necessary to identify the gaps in existing procedures, leverage the existing processes and platforms, and avoid unnecessary duplication. Then the types of incidents to be addressed must be determined accompanied by purposes of the scheme. Furthermore, the organizers have to consider which stakeholders should report into the system. Finally thresholds for reporting need to be set.

- **Engaging Cooperation.** The scheme should build on already existing arrangements for industry cooperation with the government in the field of network and information security or CIIP. At an early stage, expectations, possibilities, and value proposition of the scheme must be clearly communicated to the reporting parties. Advantages of a scheme may include: efficient and fast information distribution; access to information not available elsewhere; assistance in emergencies; and improved reaction to crisis situations. The organizers will also have to address concerns about confidentiality of submitted information and the load on resources that the reporting parties might face. Relationships with the reporting parties must be continuously built in terms of mutual trust, C-level management support, and educating the potential reporting staff.
- **Setting the Reporting Procedures.** Based on the scheme's objectives, the list of reportable information must be determined. Deadlines will have to be set for immediate, follow-up, concluding, and periodical reports. Thereafter, timely and efficient prioritization of the received reports must be ensured. In the follow-up stage, information updating and distribution, and incident response efforts (possibly including cooperation with wider public emergency response activities) become the priorities. For these purposes, it is recommended to introduce a single point of contact for reporting incidents within the eCommunications sector.
- **Managing the Reporting Scheme.** The organizers will need to introduce scheme management mechanisms ensuring that the scheme's objectives are met. Significant individual incidents should be analyzed, with corresponding follow-up steps undertaken with the incident owners, if necessary. Macro-level ex-post statistical analysis may also be desired as an efficient way of reflecting on trends. The organizers will also need to collect feedback on the scheme's functioning and respond to problems. Finally, each scheme also needs to evolve and improve on mid and long term. Long-term evolution may lead the scheme and its organizing department to play a gradually increasing role in the Network and Information Security (NIS) procedures.

The study revealed that there is an enormous wealth of knowledge and experience with incident reporting in several Member States, from which others can learn. This report summarizes the variety of approaches encountered in a way that is intended to be useful both to the stakeholders launching a new reporting scheme, and to those trying to improve the standing procedures. It also includes references to additional materials.

1 Introduction

1.1 Policy Context

In recent years, the use of public eCommunications networks has expanded rapidly to encompass a far wider range of services and applications. This transformation, expansion, and broadening of uses continues unabated. These networks have become critical infrastructure for Europe's Member States, public institutions, societies and economies.

The European Union's institutions have recognized the importance of public eCommunications networks and the need to expand the efforts to ensure their resilience. In 2006, the European Commission issued a communication on "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment" (COM (2006) 251), which was largely endorsed the following year by the Council (Council Resolution 2007/068/01). One of the main actions announced in the strategy was a multi-stakeholder dialogue on the security and resilience of networks and information systems as the Information and Communication Technology (ICT) sector specific approach under the overall European Programme for Critical Infrastructure Protection (EPCIP) adopted by the European Commission at the end of 2006.

The European Commission further adopted, in March 2009, a communication and an action plan on Critical Information Infrastructure Protection (CIIP), called "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience" (COM (2009) 149).

This communication focuses on "prevention, preparedness, and awareness" and defines a plan of immediate actions to strengthen the security and resilience of CIIs."

Data Collection Framework

In the 2006 Strategy for a Secure Information Society, the European Commission highlighted that effective policy making needs a clear understanding of the nature and extent of the challenges at stake. In that respect, the access to reliable, up-to-date and comparable data on security incidents is one element that would be needed to get a better understanding of where there is a need for actions and, as a follow-up, to assess the success of previously implemented legal, regulatory, organisational and technical measures.

In the 2006 Strategy, the European Commission proposed that a trusted partnership with Member States and stakeholders be initiated to develop an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence. The European Commission requested a feasibility study to ENISA on that topic in 2007. Further on, the CIIP communication observes that "Governance mechanisms will be truly effective only if all participants have reliable information to act upon," and then notes that

> *"....processes and practices for monitoring and reporting network security incidents differ significantly across Member States. Some do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges."*

To address this and other challenges, the CIIP communication has identified that ENISA could play a key role in conducting several tasks, including identifying good practices, and facilitating the sharing of these practices across the EU institutions and Member States

The Reformed Telecom Package

The reformed Regulatory Framework for electronic communications networks and services that was adopted in November 2009 brings a new important stone to the policy objective of developing an appropriate data collection framework with respect to the collection of reliable EU-wide data on security incidents. The new framework addresses many different issues, but within the new chapter on security and integrity (article 13), there is one provision that specifies that Member States shall ensure that telecom operators 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 their networks. Where appropriate, these authorities should inform their peers in other Member States, as well as ENISA. On an annual basis, these authorities shall submit a summary report to the Commission and ENISA of all notifications received at national level. The European Commission, taking the utmost account of the opinion of ENISA, may adopt technical implementation measures with the view to harmonising this provision on notification of security breaches.

1.2 Objectives

Given this strong commitment by the EU institutions and the Member States to the resilience of public communications networks, ENISA was asked to help Member States and EU institutions to identify good practices in incident reporting schemes.

This document addresses many of the issues that Member States will face as they debate, take stock, establish, launch, develop and harmonize their incident reporting systems at national level.

The report discusses schemes for reporting incidents that may harm or threaten the resilience and security of public eCommunication networks. It examines the whole lifecycle of a reporting scheme, from the first steps in designing the scheme, through engaging the constituency's cooperation, setting the reporting procedures, and then management and improvement of the scheme. Data protection-related incidents or data breaches are not addressed.

Due to the complexity of the subject and the diversity of the scopes, objectives, and characteristics of schemes, it is impossible to provide detailed guidance on all of the lifecycle particulars. Instead, it is intended as a reference point for all of major issues that must be addressed. It also gives insight into how other dealt with these issues and provides general guidance on the identified good practices.

1.3 Target Audience

The report aims to assist public authorities and private organizations in the EU and Member States as they implement incident reporting schemes.

It aims to support those who do not have significant experience with such schemes. Additionally, it may also serve as a tool for improvement for those managing or working with existing reporting schemes.

Furthermore, it also serves as a basis for discussion by all stakeholders about how national procedures should coordinate, cooperate and harmonize with one another under the new telecoms regulatory framework.

1.4 Methodology

This report was prepared by surveying and interviewing public authorities, network operators, IT industry players, and network security experts about their experiences, expertise, and recommendations for effective practices in planning and implementing incident reporting procedures.

A questionnaire was prepared and distributed to these experts. The experts were located primarily in the EU, though some were also located in other parts of the world, particularly in the United States. Based on the responses of experts, interviews were arranged with as many of them as possible.

The questionnaires were initially sent out in July 2009, with interviews then taking place in August and September 2009. In total, 27 questionnaires were received, 25 interviews conducted, and a total of 30 organizations contributed either in the questionnaire, the interviews, or both.[1]

In parallel to the survey and interviews, secondary research was conducted to identify incident reporting procedures in other regions of the world. Furthermore, some key experts from the cases identified during this process were contacted for verbal discussion of the practices identified through this procedure.

Following completion of this research, the results were analyzed, good practices were identified, and these findings were then prepared in the form of this good practices document.

The document was submitted to external experts for review, comments and validation. This document represents a broad consensus of a wide selection of public and private-sector experts on incident reporting schemes.

1.5 Structure

An introduction to the subject is given in the first place and then a review to the lifecycle. Each of the four lifecycle steps is reviewed in a separate chapter. Each chapter breaks down the discussion into sections. Key issues are described in details in the sections. Examples and quotes from the interviews are included where relevant to provide the reader specific examples and expert views.

Throughout the document, key good practices are presented in separate boxes for easy identification.

[1] See Appendix B for details.

2 Overview of Incident Reporting

Effective reporting procedures provide many benefits. An effective scheme can ensure that all those who need to know about an incident learn about it quickly. It also enables a coordinated response and gives those responding access to a wide pool of expertise about such incidents. It ensures that national authorities can follow up with network operators in a regulatory capacity, if necessary. And it also enables the collection of data about incidents, threats, and prior experiences to be used for analysis of threats and identification of good practices in responding to specific kinds of incidents.

2.1 Types of Incident Reporting

During the course of the research, it became clear that the term "incident reporting" is understood in very different ways. That is partly due to varying legal frameworks and national cultures of public-private cooperation, but especially due to the fact that the schemes:

- Follow varying purposes,
- Address various types of incidents,
- And involve different planning organizations.

In this section, we briefly raise these differences, which will be discussed in more detail throughout the document.

2.1.1 Purposes of Reporting

The most important distinguishing factor identified during the research was the purpose of the scheme. The three main purposes are:

- Incident response,
- Incident prevention,
- And incident rectification.

Though actual reporting schemes may represent a mixture of two or even three objectives, each of the three types is driven by a distinctive logic, understanding of which is indispensable for setting correct priorities. Details of the typology will be discussed in section 3.2.2 below.

2.1.2 Area of Reporting/Types of Incidents

Another source of differences between schemes is the primary area of reporting, which typically focus on either:

- Cybersecurity incidents,
- Or network faults.

These two areas are connected (see 3.2.1), but still they tend to involve different reporting purposes and different constituencies. As a result, the specific arrangements for reporting may differ significantly.

It should also be mentioned that for the purposes of this report, data security breaches are excluded from cybersecurity-focused reporting.

2.1.3 Authorities Managing the Scheme

Finally, the research found that the reporting schemes tend to differ according to the host organization, i.e. the organization that develops and manages the scheme. Among the types of host organisations identified were:

- Telecoms regulatory authorities,
- National or GovCERTs,
- CIP-related authorities,
- Other CERTs.

This distinction comes into play especially when the scheme's organizers consider expansion into new areas. This is due to the fact that different starting positions offer different evolution paths. Details and consequences of this distinction will be discussed in section 6.3.2 below.

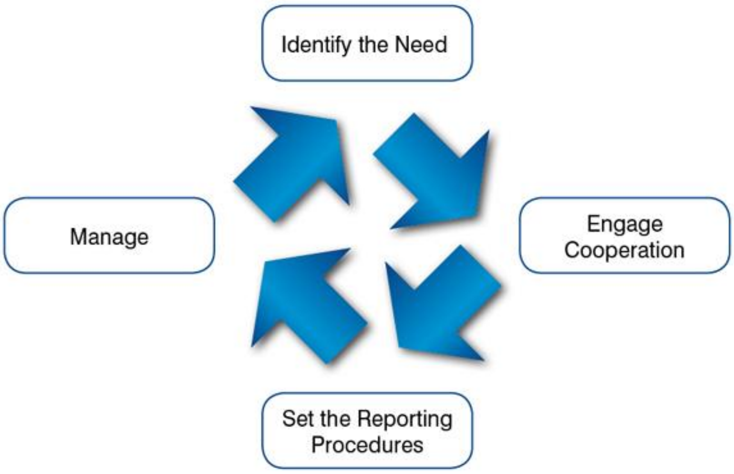
2.2 Incident Reporting Lifecycle

Planning and implementing an incident reporting scheme are challenging goals. To achieve success, it is necessary to: a) carefully and diligently proceed through many individual steps, b) working out a huge amount of detail in the process, while balancing the sensitivities of various organizations and individuals with whom you will have to work; and c) coordinate, and cooperate in both establishing and then managing the scheme. These numerous steps together form the lifecycle of the incident reporting scheme.[2]

The lifecycle could be depicted as a four-stage process. It begins with identifying the incident reporting need and setting the basic goals of your scheme. The lifecycle then proceeds to engaging cooperation of the potential reporting parties – which in fact is an ongoing effort that shouldn't stop as long as the scheme is running. The reporting procedures are then defined, enabling the launch of the scheme. Finally, every scheme needs an ongoing management that would, on one hand, provide feedback that enables adjustment of the reporting procedures, and on the other hand enable longer-term improvement and evolution of the scheme. Thus the lifecycle may naturally flow into a re-assessment of the incident reporting needs and to establishing additional reporting arrangements. Relationships between the four stages are summarized in the following figure.

[2] For the purposes of this guide, incident reporting scheme lifecycle, or shortly incident reporting lifecycle, is a summary of the activities necessary to establish, run and manage an incident reporting scheme in eCommunications. Thus it is clearly distinct from the "incident lifecycle" – an established term describing incident response processes within a CERT.

Figure 1: **The Incident Reporting Lifecycle**



Each stage of the incident reporting lifecycle contains a number of specific tasks to be carried out. We see the following tasks as crucial:

1. Identifying the Need. At the beginning of their efforts, the organizers should:

   a. Examine the status quo,

   b. Identify the scheme's goals,

   c. And define the requirements.

   Familiarity with the status quo is a necessary point of departure. The status quo contains gaps and needs that are presently not addressed and that a new scheme will have to cover or satisfy. It also contains resources that may be leveraged to the scheme's benefit, such as expert communities, industry platforms, and institutional arrangements for critical infrastructure protection and crisis response.

   Having examined the status quo, the organizers will proceed to defining the scheme's goals, which seem to consist of a twofold decision. On the one hand, the type of reported incidents (cybersecurity incidents or network faults) has to be determined, and on the other hand, the organizers will have to choose the scheme's purpose. Based on this choice, the organizers should be able to roughly outline the reporting requirements, especially: the scheme's constituency – the potential reporting parties; the reporting obligation; and the thresholds beyond which incidents should be reported.

2. Engaging Cooperation: The organizers must begin to engage with the future reporting parties in order to win their cooperation, by doing the following:

   a. Make use of the already existing arrangements and resources;

   b. Formulate the value proposition of the scheme;

   c. Raise awareness of the threats;

d. Build trust with the participants;

e. Address the private stakeholders' concerns.

Building trust with the reporting parties is one of the crucial and most difficult tasks. The organizers shouldn't hesitate to leverage the already existing cultures of cooperation and trusted relationships for this purpose. They must also clearly communicate the purpose and benefits of the scheme to the participants. To assure cooperation, the organizers should communicate with the stakeholders about their concerns and find suitable solutions.

3. Setting the Reporting Procedures: Next or parallel to engaging cooperation, the organizers will need to define the reporting procedures in detail, and introduce the means necessary to run them. They should:

a. Set reporting requirements,

b. Define the prioritization of incidents,

c. Establish follow-up procedures,

d. And develop media policies.

Reporting requirements spread across a wide area. The organizers should, of course, offer guidelines concerning the content of the report; the format of the report (standardized or free formats); time deadlines for various kinds of reports that would be submitted (ranging from a quick initial announcement to a periodical overview); and channels through which the reports should be submitted.

The organizers will also need to set mechanisms for assigning each report a priority for the follow-up stage. In the follow-up, the scheme's operation mainly consists of assembling and distributing information within and without the scheme's constituency. Apart from these procedures, the organizers will also need to arrange how to offer or mediate assistance to the participants. Last but not least, the reporting scheme organizers should have established practices for communicating with the media.

4. Managing the Scheme: When the reporting procedures are set and running, the organizers will need to pay attention to scheme management. The tasks in this stage of the incident reporting lifecycle fall into three groups:

a. Analyze and follow up on individual incidents;

b. Conduct statistical analysis of a series of incidents;

c. Examine feedback to improve and evolve the scheme.

Analysis of any significant incidents (those with a substantial impact or of an unusual nature) is the basic way of ensuring that the scheme follows developments in threats that it is supposed to face. Statistical analysis of aggregate data enables the organizers even more effectively to track trends, successes, or vulnerabilities. Results of both kinds of analysis can be discussed with the constituency. In an individual follow-up with service providers, the organizers may suggest or demand that measures are taken to prevent similar incidents from repeating in the future.

An important part of communication with stakeholders is collecting feedback on the scheme's functioning, improving the reporting procedures, or clarifying the procedures with the potential reporting staff. On a longer term, the organizers need to consider improvements in the scheme's coverage, possible amendments to its legal status, and eventually also expansion of its purpose and reporting area.

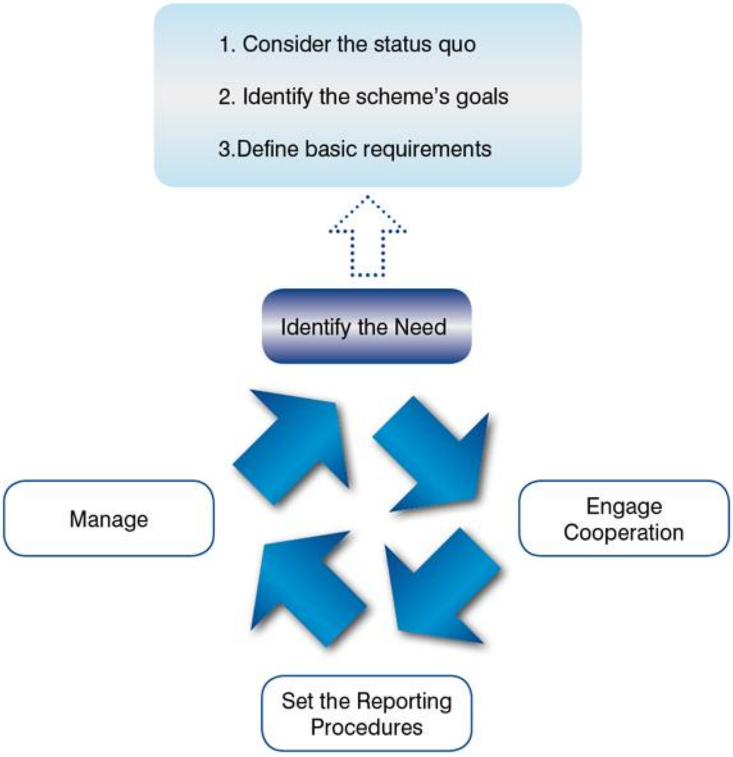
The following chapters examine each stage of the incident reporting lifecycle in detail. Throughout the text, the report identifies and recommends practices provided by experts in the incident reporting subject matter.

Where relevant, emphasis is put on positioning these good practices in their context and in the varying legal, administrative, and business cultures across nations and sectors.

3 Identifying the Incident Reporting Need

The key tasks that should be accomplished in order to cover this stage of the lifecycle are presented in the figure below:

Figure 2: **Key Tasks in Identifying The Incident Reporting Need**


1. Consider the status quo
2. Identify the scheme's goals
3.Define basic requirements
Identify the Need
Manage
Engage Cooperation
Set the Reporting Procedures

3.1 Considering the Status Quo

In order to identify the needs that the scheme should address, those formulating the scheme should first examine the status quo to identify gaps, as well as factors already in place that can aid in the establishment of the reporting scheme.

3.1.1 Identifying Gaps

Each country has its own unique environment of telecoms network operators, public institutions, legal framework, IT industry participants, critical infrastructure managers, and associated stakeholders in ICT resilience, and all of these parties may already interact in various ways. This pre-existing environment may already address some objectives, or provide a useful foundation for development of a new reporting scheme. For example:

- There may be some existing incident reporting schemes, such as industry or public CERTs, or informal means of reporting network faults to regulators.

- There may be one or multiple authorities that require some form of incident reporting and may have developed such processes already.
- There may be national policies in place for coordinating emergency response or critical infrastructure protection (CIP).

On the other hand, the existing environment can complicate matters. For example, there may be multiple institutions with overlapping mandates or contradictory objectives.[3]

In any case, this pre-existing environment should be taken into account before planning a new incident reporting scheme. Some of the incident reporting objectives may already be well-addressed by existing institutions and processes. Knowledge of such gaps and the existing environment will be critical to the development of your scheme.

- *Status quo must be taken into account before planning the reporting scheme.*
- *Gaps in existing incident reporting procedures must be identified.*

3.1.2 Leveraging Existing Processes

Taking advantage of processes and stakeholders already in place may be beneficiary for a new incident reporting scheme. By contrast, ignoring the pre-existing environment can result in unnecessary duplication of effort for organizers and for reporting parties, and resistance from would-be participants. To give a few examples:

- Avoiding duplication: Multiple reporting schemes can force reporting parties to duplicate effort during a crisis. This duplication can cause unnecessary delays. The solution is to avoid duplication where possible, possibly by creating a single reporting scheme, or simply by ensuring that the multiple schemes have clearly defined roles and responsibilities, have efficient means of cooperating where needed, and fit into a larger plan for incident response and prevention.
- Working in step with legal support and the wider community: Considering the legal status of incident reporting, and whether certain authorities have legal authority to create and manage a reporting scheme, will ensure that your scheme can either leverage that authority, cooperate with it, or at least avoid contradicting it.
- Ensuring easier cooperation and participation: Leveraging and building upon pre-existing patterns of cooperation (such as industry associations or forums) can enable faster creation of the scheme and more willing adoption by the reporting parties.
- Integration with wider plans: Since incident reporting is one part of a larger effort to handle incidents and emergencies, and to protect critical infrastructure, integrating your scheme with

[3] Stock Taking of Member States' Policies and Regulations related to Resilience of public eCommunications Networks', ENISA report, 2008, available at https://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-of-national-regulatory-environments.

the wider plans in these areas is a way to ensure that all of the above benefits are enjoyed most effectively.

Thus, those establishing a reporting scheme should leverage the status quo as much as possible.

- *Advantage should be taken by existing processes, procedures, institutions, and stakeholder interest in CIIP.*

3.1.3 Integration with Wider National Emergency Management Plans

Our research has demonstrated that incident reporting schemes in eCommunications sometimes are integrated into wider national emergency management plans, while other times they are not. The main reasons for this variation are:

- Some countries have long-established emergency management processes, into which to the reporting scheme can be integrated, while other countries have less mature emergency management plans.
- The recent emphasis by the European Union on Critical Infrastructure Protection (CIP), has brought this issue forward in recent years, making it an area of current development, with incident reporting being one small part of the whole. Thus, where incident reporting preceded these wider policies, it can only be integrated at a later date.
- Many organizers in the past developed their reporting schemes to address a need exclusively within their sector or area of responsibility (e.g., telecoms regulation, eCommunications resilience, computer emergency response) and only some connect to the national Critical Information Infrastructure Protection (CIIP) and cross-sector national emergency response strategies.

However, now that these wider national strategies are generally in place or in development throughout the EU, those establishing a new incident reporting scheme at this time mostly have the option or obligation to integrate their schemes with these wider strategies.

There are many advantages that a reporting scheme may draw from such a cooperation:

- Each reporting scheme needs a perspective for its development. That need can be well-assisted by a national strategy via listing critical infrastructure providers and determining priorities in emergency response and critical infrastructure protection.
- Public-private partnerships and expert forums that already exist as a part of the national crisis response plan may be used as a platform to build trust and win cooperation of the potential reporting parties (more in the sections 3.1.3 and 4.1 below).
- The possibility to legally sanction cooperation may be useful. If the national plan entrusts a certain organization with coordinating CIIP, that organization would likely also have the legal mandate to organize an incident reporting scheme.

__[Estonia]:__ The recent Estonian Emergency Situation Act (2009) defines critical infrastructure providers and their duties as well as public agencies responsible for critical infrastructure protection. That provides the Ministry of Economy and Communications, which is in charge of communications CI under this Act, the mandate to begin organizing a reporting scheme and demand cooperation.

- One of the roles of an incident reporting scheme is to secure coordination and communication with agencies and sectors that might be involved in the incidents. Authority of a national plan helps to establish hierarchies and organize the reporting so that the reporting parties are not burdened with parallel duties to multiple authorities (more on this in section 5.1.3 below).

Therefore, while reporting schemes can and often are effective independent of wider national emergency management plans, based on the advantages that integration provides, you should try to integrate the reporting scheme into the wider plans, where feasible.

- *The reporting scheme must be integratde with the national crisis management and CIIP plans.*
- *The legal status of a CIIP coordinator must be built up.*
- *Established PPPs and expert forums might be used so as to discuss the scheme.*
- *Systematize Cross-sectoral communication must be systematise.*
- *Multiple reporting should be avoided.*

3.1.4 Seeking International Assistance

Apart from the national CIIP scheme, also the international community can prove a valuable support to the efforts in establishing an eCommunications reporting scheme. It is important to review the situation there and ask for help wherever possible:

__CERT Community:__ The European CERT community is cooperating very closely in sharing experiences: those who are about to launch a national CERT usually contact experienced CERTs abroad for information and consultations. GOVCERT.NL is offering its lessons learned online as a "CERT-in-a-box" guide. (See the Appendix B below)

__MIMER/GLU [Sweden]__ The Swedish Post and Telecom Agency (PTS) together with some of the larger telecom operators in Sweden and the European Commission (EPCIP) are currently running a transnational dissemination project MIMER II with the participation of Finnish, Norwegian and Dutch service providers and regulatory authorities. The project should help the participants to identify their reporting needs, analyze the Swedish experience, and launch their own respective projects regarding on-going disturbances.

Our research has indicated a marked interest in internationally sanctioned experience on the side of eCommunication service providers. This can be used to attract interest in the reporting scheme.

__BKA [Austria]:__ Recently, ENISA has helped the Austrian Federal Chancellery (BKA) by providing presenters at workshops for the Austrian audience. BKA has used the workshops to raise *awareness of threats and promote subject-related knowledge among the potential reporting parties.*

- *Ask the neighbors: European expert forums or associations might be utilised for making inquiries; visits and consultations might be undertaken.*
- *International project smight be joined so as to gain expertise from others' experiences.*

3.2 Identifying the Goals

There is no single best practice in incident reporting. The best practices consist of choosing the procedures appropriate to the reporting goals, which may vary considerably. Thus the first good practice required in order to set up a reporting procedure successfully is to identify the objectives, and then build all further elements of the scheme to fit those objectives. This section should help you to do that.

- *The scope of the reporting scheme must be defined.*
- *A decision on the types of incidents addressed, and the objective of obtaining the reports must be taken.*

3.2.1 Area of Reporting

For the sake of this study, an incident is defined as an event which may harm or threaten, either directly or indirectly, the resilience and security of public eCommunication networks. Our research has shown that such events tend to be included in two different areas: that of cybersecurity incidents, and that of telecommunications network faults.

There is some overlap between these types of incidents, since telecommunications networks are dependent on a tremendous amount of IT components, so cybersecurity incidents may result in telecommunications network failure. Yet while these types of incidents overlap, cybersecurity and telecommunications resilience are anchored in different lines of business and different business cultures. And incident reporting and response procedures also tend to differ.

Cybersecurity Incidents

Cybersecurity incidents can be targeted against the network infrastructure, as well as the users of that infrastructure, such as banks, government, police, industry, and others. As a result, incident reporting and response procedures must work with both eCommunications service providers and the end-users who have significant IT assets. It has been a shared practice in the cybersecurity area to establish CERTs in order to coordinate response to incidents, distribute notifications on threats, and engage in prevention. Recently, cybersecurity tends to be subsumed under the wider CIIP policies. The incident reporting procedures concerned with cybersecurity incidents tend to focus on emergency response and failure-prevention activities.

We would like to remind again that data protection incidents, such as privacy breaches or unauthorized data disclosures are considered outside of the scope of this document.

Network Faults

In the area of network faults, the incidents may affect users and other stakeholders who require notification, but repairing the fault tends to be handled within the service provider and/or its contractors. Therefore, the incident reporting procedures concerned with these network faults tend to involve reporting from the network service providers. In contrast to cybersecurity, shared practices are more difficult to find as reporting schemes in this area can follow various objectives. These schemes are sometimes focused on emergency response, others on incident prevention, and yet others on incident rectification, or on a specific mix of these.

Combining The Two

While many schemes focus on either cybersecurity or network faults, others cover both. Whichever the choice in your case, the scheme should be designed with the specific choice of coverage in mind, so that relevant stakeholders can be involved and effective procedures put in place to meet all objectives.

- *A decision on whether the scheme will address cybersecurity incidents, network faults, or both must be taken.*
- *In the cybersecurity area, CERTs and CERT-like structures might be utilised to receive reports in order to coordinate incident response across the wide range of network operators, users and other stakeholders.*
- *In network faults area, attention should be paid to defining the scheme's purpose correctly to suit scheme’s objectives, as a focus on emergency response will lead to a different scheme than one focused on prevention or rectification.*

3.2.2 Purpose of Reporting

As noted above, reporting schemes tend to focus on one or more of three main objectives. These are:

a. Emergency or incident response,

b. Incident prevention,

c. Legal rectification.

It is important to understand the differences between the types, because much of the schemes' inner organization depends on the choice of these purposes. On the other hand, most reporting schemes would combine two or even all three purposes. Any new scheme would need to establish the major and secondary purpose(s) and combine the reporting procedures accordingly.

Reporting Focused on Emergency Response

The first type of purpose to which incident reporting is commonly tuned is responding to emergencies. These schemes aim at enabling real-time information sharing and coordination during emergency situations or time-sensitive incidents. In order to achieve the goal, it is advisable to follow several principles:

1. It is important to establish an understanding of which services are critical and need to be monitored, and make sure that providers of these services are part of the scheme. Participation in emergency-responding schemes may be limited to invited providers.

   MELANI [Switzerland]: *The Federal Strategy Unit for IT launched its Reporting and Analysis Centre for Information Assurance (MELANI) in 2004. Over time, it invited 74 companies from Telecommunications, Industry, Energy Supply, Health, Finance, Transport and Government sectors to become part of the Scheme. Selected were companies providing critical infrastructure, and especially those that were likely to be affected by a possible ICT infrastructure failure.*

   MIMER/GLU [Sweden]: *For their telco outage reporting scheme, the Swedish Post and Telecom Agency (PTS) co-ordinates and co-finances a public-private partnership formed together with the larger telecom operators in Sweden. The participants include 5–7 large telecom operators and the members of the Swedish Urban Network Association. The total infrastructure handled within the partnership sums up to about 80–90% within the country. Additional telecom operators should be able to participate in the future.*

2. For real-time information sharing, an efficient and reliable tool is crucial. Online tools such as web interfaces or GPS-enabled maps facilitate real-time information sharing. In other cases the reporting schemes may use secure communication bridges for voice and data transfers.

   ComReg [Ireland]: *The Irish telecommunications regulator, in close cooperation with the Department of Communications, Energy and Natural Resources hosts a secure communication bridge that connects key personnel at the operators and if necessary, also public emergency response agencies. In an emergency, the bridge would be opened upon request of a reporting party.*

   MIMER/GLU [Sweden] *enables three functionalities: (1) Public Function – public web page of the operator with a map that visualizes the current status of the operators telecom services; (2) Message Function – messages with information regarding the current status of the operators telecom services, forwarded via robust communications from telecom operators to the handler of the emergency call centres, SOS Alarm. SOS Alarm can then inform first responders, local agencies and other public crisis responding agencies; (3) NTCG function – support to the national crisis management group NTCG, for instance in providing secure communications tool with a number of functionalities (log-in for members; list of contacts; documents and files sharing; report/log/statistics; e-mail; chat-forum; telephony and conferencing tool). Elaborating these functionalities has also improved the internal processes of the operators (alerting the staff, suppliers, customers, etc.).*

3. Responding to emergencies is a complex task that transcends boundaries of a single sector. Organizers of an eCommunications reporting scheme will find it necessary to closely

cooperate with national and/or regional crisis management centres, and to bring in the representatives of other sectors as well, either directly or through mediation of the public crisis management. More on this kind of cooperation will be said in sections 5.3.2 and 5.3.3 below.

> ***DIRS [USA]:*** *The Disaster Information Reporting System (DIRS), run by the Federal Communications Commission, is a voluntary reporting scheme that collects reports on network outages during major emergencies. It supplies information to the national emergency communication network (National Communications System, NCS) and other federal agencies in charge of emergency response.*
>
> ***NEAT [UK]:*** *The National Emergency Alert for Telecoms (NEAT) arrangements in the UK can be connected, if necessary, to the national emergency response framework – the Concept of Operations, CONOPS. The framework defines a hierarchy of regional, sector-specific, and nation-wide public responding agencies and makes it possible for an incident report to be quickly escalated to a corresponding authority.*

- *The following must at least be ensured for reporting focused on emergency response: a) cooperation of major CI providers, b) use of efficient communications tools, c) coordination with public crisis management, and d) coordination across sectors.*

Reporting Focused on Preventing Failures

The second type of reporting focuses on reducing outages in public eCommunications networks as a means of guaranteeing a certain service to the customers. Schemes of this type aim at collecting sector-wide information on threats and putting it to use so that failures are prevented. There are two alternative approaches that can be used, each using a set of means.

1. CERTs and CERT-like institutions put emphasis on peer-to-peer cooperation, the priority being to facilitate information sharing on threats. The organizers distribute statistics and updates on current incidents, mediate consultations, organize expert forums and regular stakeholders' meetings. Of the many CERT-like structures collecting information on incidents, national CERTs, and GovCERTs are most likely to have reporting schemes that qualify for the scope of this study.

> ***BSI [Germany]:*** *The Federal Office for Information Security (BSI) is operating CERT-Bund as an example of GovCERT. It collects reports on data security incidents and network outages in government institutions and on selected networks that are regarded as part of the national CI. Among its main methods in the GovCERT function is raising awareness among the constituency, offering assistance to the afflicted parties, facilitating informal exchange of experience in trusted groups.*

2. Regulatory and supervisory bodies focus on a different priority in failure prevention. They tend to impose a duty to systematically report incidents to a single authority. Based on this, analyses and audits are carried out in order to discover potential threats and implement countermeasures.

> ***FICORA [Finland]:*** *The Finnish communications Regulatory Authority (FICORA) is running a mandatory reporting scheme with the following purpose, among others: "Incident reporting is a good tool for […] understanding the actual quality, capacity, vulnerability and resilience of the telecommunications services in Finland. […] FICORA follows closely the trends behind the incidents: what are the typical failures, most vulnerable devices, problems with fault correction activities, etc. These issues are discussed with telecom operators in the yearly meetings."*
>
> ***NORS [USA]:*** *The Federal Communications Commission organized the Network Outage Reporting System (NORS) in order to collect outage-related information after the fact, and then identify and address any shortcomings on a going-forward basis. Reporting of incidents above certain thresholds is mandatory for the operators. Data based on the reports submitted are reviewed with the industry representatives on a regular basis in order to facilitate a voluntary continuous improvement in network reliability and resiliency.*

It should be said that to a certain extent both approaches can also be combined within one scheme. Especially some elements of peer-to-peer cooperation may be added to supervisory schemes.

- *For failure prevention, peer-to-peer cooperation, recommendations and/or supervisory evaluation might be considered as the main tools to achieve the scheme's objectives.*

Reporting Focused on Rectification

The third type of purpose of incident reporting is rectification of incidents. This objective is closely related to that of failure prevention, though rather than focusing in a forward-looking way on information sharing and advice on avoiding future incidents, schemes focused on rectification tend to employ the tactic of enforcing the operator's obligations—imposed on them by telecoms laws and their license terms—to provide high-quality, uninterrupted services. By enforcing these obligations, they may achieve the goals of resilience, as well as consumer protection. In practice, they may follow up on incidents that have occurred and require that proper steps are taken so that the failure will not be repeated, or that service providers restore services to end-users more quickly. Two priorities are particularly advisable for success here:

1. It is essential that there are procedures in place to (a) collect complete information on the event from the service providers, and to (b) analyze the case with them and implement necessary changes. The cases to follow up on may be either reported by the operators or selected by the organizing authority due to their political, economic, etc., significance.
2. Following up on incidents presupposes the right to do so. The organizers of the scheme should have a legal status that entitles them to require information if necessary and impose rectification. Sanctions may be issued by the organizers themselves, or by other bodies such as the telco Regulatory Authority or the courts.

> ***Bundesnetzagentur [Germany]:*** *In Germany, resilience policy in eCommunications is significantly building on security audits and regular inspections on the service*

providers' premises. Yet in addition to this, the regulator (Federal Network Agency, Bundesnetzagentur) has the right to request information on any incidents that have come to its attention[4] *and to require briefing on the measures taken to prevent similar events in the future.*

- *For incident rectification, follow-up procedures must be established after individual incidents.*
- *A legal framework for this kind of regulation must be assured.*

3.3 Defining Basic Requirements

Having defined the broad types of incidents to be addressed and the purpose of your scheme, it is time to proceed to setting the main requirements of the scheme. We should discuss them in three batches: the reporting parties, reporting obligations and the reporting thresholds.

3.3.1 Reporting Parties

The first step is to define the reporting parties that you would need to include into the scheme. Our research has shown that there are four categories to consider. Generally, any of the following groups may be considered for all types of reporting, but usually each category is connected to one or two objectives and specific types of incident.

Large service providers. This group is the natural point of departure for all types of incident and purpose. Emergency response schemes will include them as CI providers in eCommunications; failure prevention and rectification schemes will prioritize them as those affecting most customers. They will be important for both network fault and cybersecurity areas.

Smaller service providers. Smaller SPs may be excluded from emergency response schemes, if their services are not considered of critical importance. They usually are included in failure-prevention and rectification schemes because they are providing service to customers. Smaller service providers are an important part of the reporting constituency in the area of cybersecurity. Because of scaling and resource-related issues, the smaller SPs are sometimes only obliged to report major incidents on their networks – especially in the network faults area.

> ***FICORA [Finland]:*** *"As a regulator, FICORA must take into account different characteristics of different operators so that the obligations given with regulation do not inhibit competition and service offering. The prioritizing of incidents helps to solve this challenge; large scale incidents can only happen to bigger players who can handle their heavier obligations."*

Other partners. For cybersecurity, incidents on the networks of large end-users such as corporations, government offices etc. are also important. Key IT equipment or software vendors and other CERTs may also be encouraged to report. In emergency response reporting, CI providers and others involved in emergency response from other sectors would be asked to actively exchange information.

[4] In many cases Bundesnetzagentur learns about incidents through notifications made by citizens or the press.

The public. Spontaneous reports on outages from end-users, media etc. may be a useful source of information for any scheme, as they could point to outages that would otherwise have slipped under the radar. Rectification-focused schemes sometimes pick sensitive cases to follow from similar reports. Organizers of all reporting schemes might wish to invite reports from the public in order to be aware of complaints or rumours that they would need to address publicly.

- *Large network operators must be involved into every kind of scheme.*
- *Smaller network operators may be excluded or charged with lesser reporting requirements.*
- *For cybersecurity reporting area and for CIIP, key end-users should be reporting their problems.*
- *Key technology vendors might also be included, as they will hold significant expertise about vulnerabilities and solutions.*
- *Openness to spontaneous reports from media and the public is useful as another avenue of reporting.*

3.3.2 Reporting Obligation

With an idea of which reporting parties should be involved, it is necessary to start reflecting on how to engage their cooperation.

Our research has shown that a few of the reporting procedures in place in Europe are mandatory, such as the systems maintained by telecoms regulatory authorities in Finland and Germany. Most schemes, though, are voluntary.

It is interesting to note that respondents with mandatory schemes emphasized that a key to the success of their scheme is still to build trust and a spirit of voluntary cooperation, while several of those with voluntary schemes stated a desire to obtain some legal reinforcement to their schemes.

Legal backing is substantial for rectification-focused schemes. Other schemes may, or may not work with a legal obligation to report.

Legal phrasing of the obligation usually amounts to a small legal clause in a telecoms regulatory act or in operator licenses saying that the service providers are obliged to report, to cooperate, or to rectify failures. The organizing authority then develops policies to implement this clause. In accordance with the national legal system and legal culture, these policies may be either formal regulations or individual agreements with the reporting parties. These policies may change as the scheme evolves.

> ***FICORA [Finland]:*** *According to the Communications Market Act, a telecommunications operator shall immediately notify FICORA (the Finnish Communications Regulatory Authority) of a possible significant fault or disruption in a communications network or service. The Act on the Protection of Privacy in Electronic Communications adds other duties to the operators, such as notifying FICORA of significant violations of, or threats to information security on their networks or services, and of measures undertaken to prevent the reoccurrence of such violations, threats, faults and disruptions. Based on aforementioned acts, FICORA has issued a specific regulation in order to describe the details of the incident reporting scheme.*

Obligation is not enough. Even where reporting is mandatory, the experts we interviewed emphasized the need to engage stakeholders' support and to build trust with the reporting parties. Unless convinced of the purpose of the scheme, and confidential handling of the information submitted, the reporting parties might not cooperate as much as necessary for the scheme to run smoothly.

> ***MIMER/GLU [Sweden]:*** *The participation is voluntary. The coordinator and co-financer of the scheme is the Swedish regulatory authority PTS, which has the power to impose obligations on service providers. The scheme has been put in operation through several years of consultations and joint coordinated development, implementation, testing and evaluation. The partners have been aware of the fact that MIMER was a possibility for the eCommunications sector to develop a joint solution tuned to the prerequisites of the sector; unless they acted together, a demand might arrive later from the society and result in a regulatory decree.*

In emergency response-focused and failure-focused reporting, much of success depends on a trustworthy relationship with the reporting parties. The organizers may begin building cooperation and trust even without a legal obligation to report. Later in the lifecycle of the reporting scheme, they may consider improving the legal anchorage of the scheme.

> ***CERT-EE [Estonia]:*** *Estonia has a track record of efficient informal cooperation among the key players in IT security incidents. Recently the country has introduced legal codification of CIIP, including the obligation to report incidents. On the system level, the benefit is to bring critical infrastructure protection on a common platform with longer-term goals. With respect to the reporting scheme itself, the organizers hope to improve crisis communication, raise awareness of threats, and expand coverage of the scheme.*
>
> ***BKA [Austria]:*** *The Federal Chancellery (Bundeskanzleramt, BKA) is still waiting for legal updates that would improve its position to cooperate and share information with other organization as a GovCERT. Nevertheless, the organizers have already begun with building expert communities, spreading awareness of the threats and establishing their status as a trusted partner.*

Article 13 of the recently adopted reform of the Telecommunication Package mandates competent national authorities to establish and manage national incident reporting schemes. “The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with the view to harmonizing policies at pan European level.” This means that the schemes should be mandatory.

- *Legal backing for rectification-focused reporting must be ensured.*
- *The legal obligation must be formulated in general terms; follow up with specific implementation.*
- *Obligation is not enough to ensure an effective scheme on its own; co-operation with reporting parties must be maintained.*

3.3.3 Reporting Thresholds

The previous sections helped to clarify the array of reporting parties and to set the legal status of reporting (obligatory or not). But behind every scheme, there should be a clear idea of what incidents should be reported, what threshold should trigger the reporting mechanism. Whether the scheme's organizers wish to make these thresholds formal and binding, or not, we strongly recommend that there be a detailed idea of the criteria that make an incident eligible for reporting.

Defining thresholds is a very difficult task. Below, we just present a number of important insights that might influence the decision on the appropriate thresholds.

Questions for the Organizers

In order to define the thresholds after which incidents should be reported, three types of factors need to be taken into consideration:

- What is the purpose and area of reporting?
- What is the organizers' capacity to handle the reports?
- What burden does the threshold impose on reporting parties?

These will be discussed in more detail as follows:

1. Purpose and area of reporting as defined above directly influence the reporting thresholds. If the plan is to rectify major incidents, there is no use for reports of small-scale incidents. If the scheme aims at preventing failures through statistical analysis of trends, incidents of all sizes may need to be reported. In order to meet different priorities, some interviewed organizations use real-time reports for larger incidents, and aggregate statistical reports on smaller incidents.

   FICORA [Finland]: *The Finnish Regulatory Authority currently considers setting differentiated thresholds. The topmost category would require an almost immediate reporting (within one hour) while the lowest category would only be included in periodical reports.*

   Theodore Puskas Foundation [Hungary] *operates two duty services: CERT-Hungary for cybersecurity incidents, and the National High-Level Service for Communications and Informatics for communication incidents (on behalf of the national Regulatory Authority, NHH). Both duty services operate 24/7, receiving instant reports on communication service failures and periodical reports on cybersecurity related incidents. Instant reporting would concern much lower number of incidents, but would result in immediate follow-up action such as issuing alerts, escalation to the NHH, contacting emergency response authorities, etc. Periodical reports are used for statistical analysis, evaluation of trends etc.*

2. The organizing authority's capacity to handle the reports is important, too. Many reporting schemes use only a small number of staff, who might be unable to prioritize incidents if inundated with low-threshold reports. It is not advisable to invite a large volume of reports

unless the organizers have at their disposal either a large volume of human resources, or an automated reporting tool (see section 5.1.1 on automation).

3. Finally, organizers need to be aware of the burden they are imposing on reporting parties, and consider whether that is reasonable given the likely level of commitment they will obtain from reporting parties. If the threshold is too low, reporting parties will likely resist and fail to submit all reports or submit only incomplete data.

- *The targeted reporting thresholds should be adjusted to the scheme's purpose, such as higher thresholds for emergency response and lower thresholds for statistics, failure prevention.*
- *A large volume of reports should be avoided when there is a lack of extensive human resources or automation.*
- *High thresholds are recommended in the beggining, and once the scheme and staff are in place and working effectively, organizers can consider whether lower thresholds would be beneficial.*

Threshold Criteria

Depending on the purpose and area of reporting, the following indicators may be used as thresholds for requiring a report. As most schemes combine several purposes, you might also wish to combine the threshold criteria.

Need of assistance. In the cybersecurity area and in emergency response, the minimum functionality of a reporting scheme is to react where the reporting parties declare they cannot manage the situation themselves. Upon the report, the scheme's organizers may start arranging assistance in removing the problem. According to a similar logic, the reporting parties may also be asked to also submit reports or alerts on threats that are manageable on their own network but might be beyond other operator's capacities.

> ***CERT-LT [Lithuania]:*** *Threshold set for the mandatory reporting is when the ISPs cannot handle the incident or might see a potential risk for others.*
>
> ***NEAT [UK]:*** *Sharing information between operators on an emergency communications bridge enables the operators to share information on the extent of the emergency and ask for assistance (mobile exchanges etc.) for handling incidents if they don't have sufficient resources at hand. Operators participating on this call are signatories to a Memorandum of Understanding.*

Impact on critical infrastructure or on other CI providers. In emergency reporting schemes, the decisive factor may be whether certain critical services are affected (e.g., the emergency call number) by the incident, and whether other CI providers (hospitals, airports, water suppliers etc.) are affected by it. This may result in a list of critical services and customers to be taken into consideration by the reporting parties. Unavailability of a service may also be reported by the end-users.

MELANI [Switzerland]: *MELANI is a reporting scheme covering national CII in Switzerland. Any member of the scheme may report an incident that in his/her opinion impacts other users and request a communication bridge to be opened. The reports may be submitted by CII providers but also by the end-users from other CI sectors.*

Impact on customers. Failure-prevention-focused and rectification-focused schemes tend to be focused on the impact of an incident on users of the service, so the reporting thresholds would also be based on the impact on those users. The criteria tend to be more or less complex, but in the most recommendable cases, three aspects are taken into consideration:

a. The number of customers afflicted;

b. The area afflicted (region, a certain number of municipalities and towns);

c. Duration of the outage.

NORS [USA] *requires reports, i.e., on outages of 30+ minutes that affect at least 900,000 user minutes (calculated as outage duration x No of customers); or at least 1,350 DS3 minutes (calculated as outage duration x No of actual calls at the moment of outage).*[5]

FICORA [Finland] *is currently proposing a new categorization of outages ranging from Class A (highest priority) to Class D (lowest priority). In telephone and broadband, the thresholds range as follows.*

- *Class A: 100,000+ telephone service users or 200,000+ broadband service users or 60,000+ km2 area affected. Etc… down to:*
- *Class D: less than 1,000 telephone or broadband users, less than 10 base stations of a wireless network.*

In addition to that, outages in wholesale services may be included for their effect on end-users.

ComReg [Ireland] *requires reports on both access tier and wholesale services. The reporting is mediated through the incumbent, which in turn reports to ComReg.*

Social, political etc. impact of the incident. Predicted or perceived importance of an incident for social, political and economic life of the country may be used as a threshold, too. That is most likely to happen in a rectifying schemes, where the organizing authority might request reports on publicly sensitive cases. Similarly, the service providers might spontaneously submit report on a sensitive case in order to avoid later criticism for not having acted upon it.

- *The need of assistance might be considered as a criterion for emergency response and cybersecurity.*
- *The impact on CI providers might be considered as a criterion for emergency response.*

[5] *See the Code of Federal Regulations, Title 47, Volume 1, Part 4, Sec. 4.5-4.9, 4.13 for details.*

- *The impact on customers might be considered as a criterion for failure prevention and rectification.*
- *Social and political impact of an incident might be considered as a criterion for rectification.*
- *Impact on customers is a combination of the the number of customers affected, the area, and the duration of the outage.*

Formalized, or Not?

With a clear idea of the reporting parties and the thresholds it is important to consider whether these thresholds should be formalized or not. Should the organizers publish a set of thresholds with which the reporting parties will be expected to comply or should they rely on informal understanding and one-to-one arrangements with the reporting parties? Again, the response varies according to the purpose of the reporting scheme.

Emergency response schemes often do not have formal thresholds. More often than not, the organizing authorities prefer to rely on responsibility of the reporting parties, and on their assessment of the situation and its impacts. The respondents often emphasized that the scheme needs to be flexible:

> ***[Regulator]:*** *"The nature of the business is to face the unexpected."*

Failure-prevention schemes may benefit from formal thresholds. From the interviews, it became clear that formal thresholds tend to be in place already for such schemes, and other organizing authorities consider that there would be benefits to formalizing their current informal arrangement. The main purpose is to receive complete information on the incidents that are relevant to the overall condition of the public eCommunication networks.

> ***CERT-EE [Estonia]:*** *As already indicated, until recently Estonia has successfully used an informal cooperation among the key IT security players in order to respond to incidents. CERT-EE is in the process of implementing a mandatory system with formal thresholds, in order to expand the coverage to all relevant organizations, including smaller service providers and other organizations that so far have remained outside of the cooperation. The organizers believe that it is useful to complement mandatory reporting to the state also with information exchange between private stakeholders.*

There is space for spontaneous reporting even in the failure-prevention type. Members of CERT-like communities often submit information they think might be helpful to other stakeholders; network operators may report spontaneously in order to meet their social responsibility, warn customers, or based on their one-to-one agreement with the regulator. The organizers may consider postponing formalization in cases when evolving nature of the incidents makes it difficult for the stakeholders to reach consensus on definitions and thresholds.

Formal thresholds seem fully eligible for rectification-focused reporting schemes, but an informal perception of sensitivity of the incident seems even more important here. As remarked previously, the service providers might feel obliged to report in order to assure the public that appropriate action is being taken, or alternatively the regulatory authority may request a report upon noticing an outage due to media interest or reports from the public.

> ***Political sensitivity:*** *A number of organizers of reporting schemes mentioned that they would require reports submitted if an incident came to the attention of the political representatives (Parliament etc.), or the public itself. They also tried to reach understanding with the stakeholders to report such incidents spontaneously, in order to meet the responsibility that both the reporting parties and the scheme organizers had towards the public*

> ***MinEcon [The Netherlands]:*** *"Certain criteria [for reporting] have been selected. When an incident meets the criteria it has to be reported by the provider. On the other hand the provider should also report smaller incidents if he foresees heavy political or media attention."*

Whether there is a formal threshold or not, the organizing authority should take care that there is an understanding among the reporting parties of what should be reported and why. Numerous respondents emphasized the importance of reaching this kind of understanding through intensive communication with the stakeholders: individual consultation, follow-up on their first reports, seminars, industry forums etc.

> ***MinEcon [The Netherlands]:*** *The Dutch Ministry of Economic Affairs runs a reporting scheme with no formalized thresholds. When launching it a several years ago, it ran a series of one-to-one-talks with service providers. They discussed impacts of possible incidents and arrived at an understanding above which levels should the incidents be reported – concerning area or number of subscribers affected, social and economic impact of the incident, etc. They also informally reviewed the SPs' business continuity plans and agreed additional criteria such as the Ministry being notified of any incident that the SP's internal procedures escalate to C-level management.*

> ***FICORA [Finland]:*** *"A regulator (such as FICORA) must make sure that all the players identify properly their obligations as a telecom operator. Especially small players do not always have good enough understanding of what is expected [from them…] Continuous reminding and discussion of best practices for incident handling scheme is needed with the operators."*

- *A shared understanding of what should be reported and why with must be cultivated.*
- *Particular focus on flexible situation assessment must be given in emergency response schemes.*
- *Aim at formalization in failure prevention schemes.*
- *Spontaneous reporting must be stimulated as a means of identifying additional needs/commitments and proceeding towards more standardized reporting.*

4 Engaging Cooperation

When the key parameters of an incident reporting scheme have been identified, the organizers need to engage cooperation of the potential reporting parties. In this context the question arises again whether and how to combine obligations and incentives: Should liabilities be imposed, and if so, which ones? And what kind of benefits should be offered to the reporting parties?

Because of the great variety of European legal and policy-making cultures, no detailed guidance can be offered on how to arrange a legal foundation for a reporting scheme. Until now, public incident reporting schemes have mostly enjoyed certain legal foundations simply because of their organizers' status as national CIP authorities, national regulatory authorities, ministries or adjacent bodies, etc. Laws and sub-legal norms also establish general obligations to abide by the national CIP or CIIP plans and to cooperate with telecommunications regulatory authorities.

Throughout this section, and in fact throughout the whole of this document, incident reporting appears as a form of cooperation involving both determined organizers and a committed constituency. So far as legal backing is understood as a support for the former, it is useful – which probably is the reason why there is a certain movement towards strengthening the legal status of the reporting schemes in Europe (see section 6.3.). On the other hand, our research has shown that the constituency's commitment is hard to win by legal obligations solely, and there are several cases where it has been built in their absence.

Our research has singled out no particular incentive or premium attached to participation that would provide the key to the stakeholders' cooperation. Instead, a complex mix of issues emerged that influenced how the reporting scheme would be perceived by the constituency. The main components are awareness of the threats that the scheme is designed to face; a clear value proposition; trust between organizers and stakeholders; and a set of particular concerns that private stakeholders may have with participation, especially confidentiality issues.

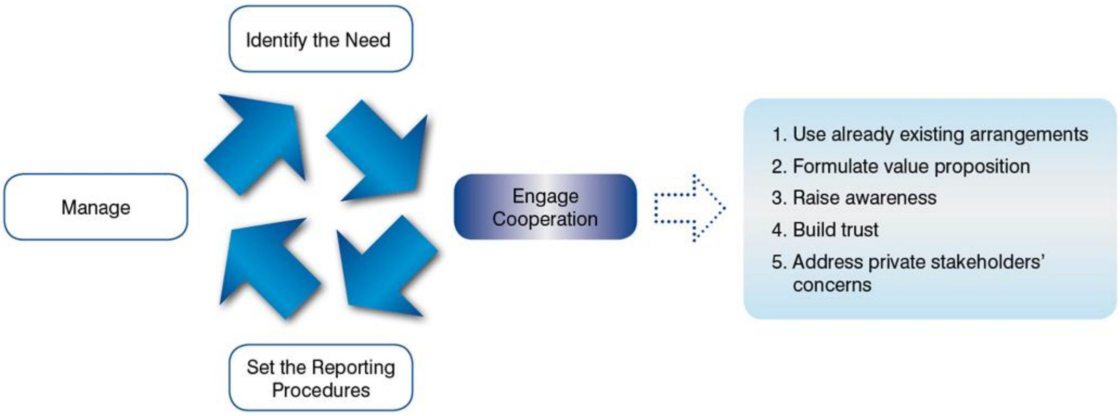
This combination of influences points to the fact that the best incentive is a well functioning reporting scheme itself. The stakeholders are must willing to participate, if they trust the scheme and are convinced of its usefulness for the national CIIP, including their own business continuity processes.

Trust and commitment are not easily generated, though, and therefore engaging and maintaining cooperation is a long-term process that should not be underestimated. This section will discuss the best practices in this area by issue and in an order in which they are most likely to pop up when organizing a new scheme. These issues include:

- Using already existing arrangements;
- Formulating the scheme's value proposition;
- Raising awareness of threats;
- Building trust with the stakeholders; and
- Addressing the private stakeholders' concerns.

Unless stated otherwise, the recommendations are meant for all areas and types of reporting.

Figure 3: **Key Tasks in Engaging Cooperation**


Identify the Need
Manage
Engage Cooperation
Set the Reporting Procedures
1. Use already existing arrangements
2. Formulate value proposition
3. Raise awareness
4. Build trust
5. Address private stakeholders' concerns

4.1 Starting with What Already Exists

Once again, the organizers of a reporting scheme are advised to reflect upon what their starting point is. This time, they should be looking for already existing arrangements that can facilitate their tasks. Our research has shown that there are two kinds of resources to draw on:

1. Already existing relationships and institutions.
2. Nation- or sector-specific cultures of cooperation.

4.1.1 Existing Relationships

When soliciting support for an incident reporting scheme, the organizers should first reflect upon any institutions that already are in place in their sector, and make the best possible use of these. Our research has indicated a number of platforms:

- Previous reporting schemes, if any;
- Industry expert forums;
- Public-private partnerships;
- Regulatory groups;
- International networks and events.

Especially in cybersecurity, private initiative may be ahead of the public one, so using private forums as collaborators or points of reference makes sense.

> ***Cybersecurity [General]:*** *A number of US-based respondents mentioned that private companies were quite advanced in coordinating IT Security issues through associations such as IT-ISAC. In Europe, e.g. CERT-EE mentioned that prior to its establishment in 2006, private companies already had been coordinating between themselves in IT Security.*

A successful reporting scheme requires a lot of communication with the stakeholders and potential reporting parties during the preparation stage, the launch, and the ongoing management of the scheme. Communication requires trust, and a platform. For both, it is beneficial to depart from already existing relationships and possibly to branch out.

> ***MIMER/GLU [Sweden]:*** *MIMER was born out of the activities of a sector-wide public-private partnership in crisis handling and continuing on previous trusted relationships in the sector; an important role was played by the National Telecommunications Crisis Management Coordination Group (NTCG), founded in 2005 and organized by PTS and the telecom operators. One of the first decisions of NTCG was that in order to improve the crisis response capacity and cross-sectoral cooperation, a common situation awareness regarding electronic communications was needed. For that purpose, MIMER was formally established in 2006; consultations, technical development, implementation, tests and evaluation have been continuing since then. In 2007, 2008 and 2009 different functions in MIMER have been put in operation.*
>
> ***ComReg [Ireland]:*** *The Irish Regulator has positive experience with anchoring the reporting scheme to expert groups that are competent in addressing their respective kinds of threats. It also recommended using regulatory groups as discussion platforms and consensual decision-making bodies during the establishment of a reporting scheme.*

- *Map the already existing arrangements and build on them.*

4.1.2 Culture of Cooperation

Reporting schemes will not be the same in all countries, not only because of different purposes and areas but also because of the variations in the business and administrative cultures. Our research has shown that the diversity needs simply to be accepted as a fact. On the other hand, all cultures contain a mode of cooperation that, if correctly identified, may be used to the reporting scheme's benefit. For example, respondents indicated the following in various places:

- Spontaneous compliance with the law embedded in the national and legal cultures;
- Feeling of responsibility towards the society and respect to the institutional representatives of social interest:

  [UK]: *"We believe in being a good citizen."*

  [Finland]: *Our main motive is "that the country we operate in is in good shape."*
- National culture of informal communication and cooperation, and communication among representatives of important social interests;
- Emphasis on flexibility and efficiency in solving problems;
- An established preference for pragmatic cooperation rather than jumping right to *"getting the lawyers involved".*

- *The local culture of cooperation must be leveraged as long as it facilitates cooperation.*

4.2 Value Proposition

> ***[Reporting Scheme Manager]:*** *"People are now waiting to see what we have to offer."*

In convincing the partners to participate, it is important that the organizers are able to formulate a value proposition. Being clear about the purpose of the system, mutual possibilities and expectations, also helps to establish trust and avoid suspicions between the participants and the organizing authority. Our respondents have mentioned four areas perceived as particularly attractive:

1. In emergency situations, the information about an outage delivered via reporting scheme may arrive substantially earlier than else. The targets of importance to the participants may vary: from suppliers to key customers, other CI providers, down to public and consumers.

   > ***MELANI [Switzerland]:*** *The experience says that within MELANI, an information on CI failure is delivered in close to real time to the concerned parties, while without the system, the reaction time may be protracted and coordination between other possible targets within the CI is not guaranteed.*

2. Especially at the onset of the process, the organizers might need to provide more information than they receive in order to convince the reporting parties. The information offered as an advantage should be of a kind that the stakeholders cannot obtain elsewhere, i.e. government data and insights.

   > ***[Security Software Vendor]:*** *Even as an expert company self-sufficient in terms of IT security alerts, the company would be interested in more information on general emergencies such as pandemics etc. There are several possible advantages: to prepare for emergencies we haven't considered so profoundly, because "you don't know what you don't know"; to better understand the scope of the challenge; to learn about best practices in order to improve the company's business continuity processes.*

3. The reporting scheme may mediate information that private companies might never be able to share. It may capitalize on the level of trust it had established with the reporting parties and offer consultations, comparisons and standards based on submitted reports. Respecting the stakeholders' concerns with confidentiality by anonymizing the information shared is an obvious condition.

4. Especially in cybersecurity, it is quite usual that a CERT's activities considerably boost emergency response capacity of the constituency. But any other scheme containing emergency response elements is capable of offering similar advantages.

- *Expectations, possibilities, and value proposition of the scheme should be formulated clearly and communicated to the stakeholders.*
- *Particular incentives for participation must be given: efficient and fast information distribution; access to information unavailable elsewhere; role of an information broker; assistance in emergencies; improved reaction to crisis situations.*

4.3 Raising Awareness

For engaging commitment to the reporting scheme, it may be necessary to increase awareness of threats that the scheme is facing. Sadly enough, a great help there are disasters, which bring the public opinion and the service providers to realize the impact of incidents, the profundity of cross-sector dependencies, etc. We have seen throughout the research that several reporting schemes started after major attacks on national infrastructure, especially after 9/11, and the April/May 2007 DDoS attacks in Estonia. If the scheme organizers can react to an incident and show the significance of their services, it is a great asset.

> ***BKA [Austria]:*** *As a lesson learned during the 2009 Conficker crisis, GovCERT.at has begun to assemble a "voluntary fire brigade" from its contacts within the public administration – i.e., a team of technicians that could reset all computers of an organization as soon as possible in case of an emergency. This backup capacity can be requested by any affected organization or by the CERT staff in case of need.*

As the interconnection of eCommunication networks advances, the industry recognizes the need to share information. Awareness of the threats and of reporting as a way to help face them has been growing gradually.

> ***IT Vendor [USA]:*** *We observe over the years that talks in the IT sector have been shifting from "why we can't share information" to "what information we need to share".*

Relying on sudden events and general trends of course would not be enough. Awareness can be cultivated only through pro-active communication focusing on two key levels in the reporting organizations: top-level management and the potential reporting staff.

On one hand, it is important that the C-level management understands and supports the goals of the scheme. For that purpose, regular meetings and consultations may be used.

On the other hand, we also heard during the research that the staff responsible for reporting within the participating organizations (network managers etc.) might not report either because they are not aware of the existence of a threat, or because they do not prioritize incidents in their day-to day business. To avoid such problems, the respondents recommended workshops for experts and middle-range managers, newsletters, web pages with reference information, even using instruction DVDs.

> ***BSI [Germany]:*** *In fulfilling the function of GovCERT, the Federal Office of Information Security (BSI) holds meetings at the CIO level three times a year to discuss BSI's services and the participants' concerns. It also organized a project group composed of middle-range managers directly responsible for the reporting; the group meets four to five times a year to discuss technical arrangements of the reporting scheme. In addition to that, BSI is publishing a regular IT security newsletter with statistics, expert assessments, recommendations, advice, user comments, etc. Pitching the feedback and deliverables to convince the reporting parties of the benefits of reporting for themselves is considered "difficult but crucial".*

- *Learning from experiences of major incidents is useful, but not enough. Advantages of the scheme should also be demonstrated to the participants.*

- *Management support must be assured.*
- *Reporting staff must be trained.*

4.4 Building Trust

Building trust with the reporting parties is a long process and at the same time a crucial condition of a successful reporting scheme. Some tips on this issue:

- It is possible to capitalize on trusted relationships that have been built previously, within other institutions.
- Building trust is a personal business – it is necessary to maintain personal contacts, meet the contact persons in the reporting organizations, organize workshops and regular face-to-face meetings both formal and informal.

  > ***MELANI [Switzerland]:*** *The organizers of the scheme made the experience that building up communications is "a time-consuming business" where the public authority has to put repeated efforts into establishing and maintaining personal contacts. If a contact person leaves a CI operator, the time and effort must be taken to find and establish a contact of the same quality; therefore, it appears useful to have more than one contact person within a single company. In principle, tangible and valuable information must be shared with the CI contacts to establish a working, trusted collaboration.*

- In their interactions with reporting parties, the organizers should be able to differentiate between those organizations that already have a track record of trusted cooperation, those who don't, those who show interest in cooperation, those who need support or consultations, etc. The fact that the organizers are serious about the project and are engaging support of other similar organizations will help.

  > ***FICORA [Finland]:*** *Organizers of the Finnish reporting scheme said that it was easier to win cooperation from big operators with a long history of relations with FICORA. Smaller service providers and fresh entrants to the market might have been reluctant, even hostile to the idea of reporting at the beginning. With step-by-step integration to the scheme, many began to see the added value of exchanging information, too.*

  > ***MIMER/GLU [Sweden]:*** *During the introduction of MIMER, the Swedish Post and Telecoms Agency (PTS) observed that one important thing needed for the operators to decide to publicly display the network disturbances (or "outages") on a map on their respective websites was that virtually all other large telecom operators also made the same decision. Within a year from launching the project, a general hesitation had disappeared and the operators were instead 'competing' who launches the website first.*

- The reporting parties and other partners (i.e., organizations generating information as well as those receiving/using it) should be involved in developing the reporting scheme. That on one hand helps to build trust and confidence regarding the project, but on the other hand it also adds value for the participating organizations. Many service providers are interested in building relationships with public authorities, influencing national policies and coordinating their reporting mechanisms with those public. Security experts within those private companies may be looking forward to consultations with public authorities because they validate their work.

> ***[Network Operator]:*** *One major international operator seems to have overcome many issues in building trust with public authorities. The company currently sees as an advantage to be involved in formulation of national policies and to have the possibility to tune the company reporting templates with those national. It is happy to maintain close contacts with relevant officials at the public authorities and to foster the understanding of how the company solves network problems. The company encourages its local subsidiaries to actively participate in national CERT communities and to cooperate with the authorities.*

- Much of the trust-building effort involves addressing the concerns that reporting parties might have about the introduction of a reporting scheme. These concerns are discussed further in the next section.

Trust-building is the top priority for incident reporting. It requires a great deal of effort over an extended period of time, but it is essential for most schemes, especially those focused on prevention and response.

- *Build on previously existing trusted relationships.*
- *Personal contacts in the reporting parties must be developed and maintained.*
- *An individual, differentiated approach to the partner organizations must be used.*
- *The reporting parties must be involved in the scheme's design and development.*

4.5 Addressing Private Stakeholders' Concerns

Our research gave us insight into some concerns that the private companies might have with entering an incident reporting scheme. The overview below puts emphasis on large operators and vendors to whose opinions we've had privileged access. The feedback generally falls into two categories:

1. Issues with confidentiality of the information submitted;
2. Issues with resources necessary to participate in the scheme.

4.5.1 Confidentiality

First and foremost, private companies are concerned about the confidentiality of information that they report to the organizing authority. Disclosure of what has been considered confidential information may do substantial damage to their will to cooperate. To overcome that issue, the general good practice is to give a clear idea of what will happen with the information that the participants submit, and provide guarantees that this procedure will be respected. The research has indicated several issues that the private-sector participants tend to be especially concerned about, including:

- Regulatory interventions,
- Business competition,
- Public image,
- Communication with large customers.

Service providers are concerned with any regulatory interventions that their reports could trigger. This might lead to serious consequences in emergency reporting; therefore, many respondents recommend separating the reporting loop from official communication with authorities charged with regulatory or punitive functions. More details on this issue will be discussed in the next section.

Service providers might feel comfortable to share certain information with the organizing authority but at the same time they would be anxious not to reveal this to the competitors. That goes particularly for topology of services, and for the service provider's capacity (or not) to provide services in a certain area. On the other hand, the service providers are interested in sharing best practices and solutions even with competitors.

> ***[Network Operator]**: A case was quoted to us when a service provider felt uncomfortable about the unexpected disclosure of the location of several of its core network components, which information the operator felt could give its competitors an advantage in winning certain customers.*

With respect to public communication, the reporting parties regularly wish to be in control of any information about their operations that goes to the media. To respect this concern, the respondents recommend either consultation with the reporting parties, or at least anonymizing any information that the organizing authority communicates to the public.

> ***[Regulator]:** In all media relations, one regulator stated that it refrains from revealing any information on companies or private persons, unless the party concerned has made that information public.*
>
> ***[National CERT]:** One national CERT anonymizes the information submitted to the media, never naming individual companies. The purpose is to keep the trust of the ISPs.*
>
> ***[Incident Reporting Scheme Manager]:** "If publications or press inquiries concern a member, this will be of course discussed with those responsible (for example the news service) of the involved company."*

The operators may be interested in participating in order to improve relations with their big customers. Some customers perceive participation in an emergency response scheme as an indication of the provider’s commitment and ability to quickly restore services. Further, customers who are participating in a reporting scheme or an information sharing platform together with the service providers can be "educated" on certain threats so that, for instance, they accept that it was not possible to restore the service earlier.

- *Clear rules on how the submitted information will be treated must be established*
- *Emergency reporting must be separated from the information collected for regulatory purposes.*
- *Confidentiality on network topology and other information that might be used in business competition must be maintained.*
- *Information released to the public must be anonymous.*
- *Incident reporting might be used as a channel to improve communication with customers.*

4.5.2 Resources

Our research has shown that direct expenses of reporting are not the main concern of private stakeholders, though covering some of the expenses may be used as an additional incentive. More interesting, from the service provider's point of view, are resources for resiliency-related issues.

In the network fault area, service providers can be motivated to actively participate in reporting if they see that public resources would be made available to aid response to emergencies or upgrade their network resilience. Information sharing and peer-to peer cooperation is also seen as a way to improve resilience without increasing the costs.

> ***[Network Operator]:*** *Sharing solutions with other operators helps in a situation where the number of incidents grows, while resources stay the same. Especially companies with similar networks and a lot of interdependencies may benefit from sharing with their competitors. […] You also have to report when you request help from the public authorities or other operators.*
>
> ***[Regulator]:*** *The operators are interested to see the regulator intervene so that they don't have to bear all the costs.*

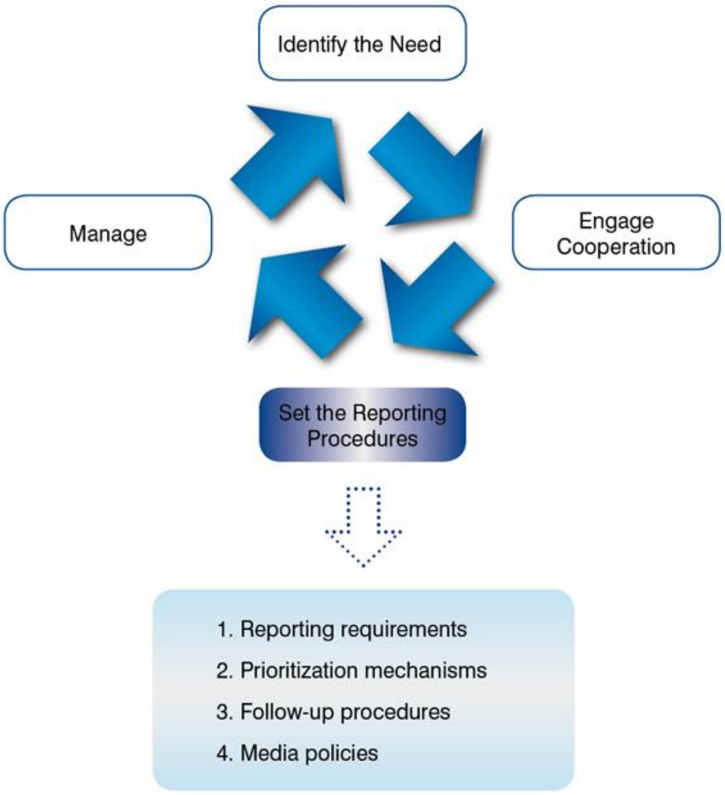
But the main resource-related issue that emerged in the research concerned human resources engaged in solving an incident on a service provider's premises. Respondents repeatedly pointed to the importance of the staff not being overburdened with reporting duties while responding to an incident. The usual practices to address this issue on the scheme organizers' side involve requiring a brief report on the incident opening and a detailed report afterwards and introducing a single point of contact to avoid parallel reporting to multiple authorities or stakeholders. In case of an incident, the scheme would distribute the information to all concerned parties based on a single report. These means will be discussed in the next section.

- *Incident reporting is resource demanding task. Reporting parties' HR economy should be taken into account when setting the reporting requirements.*
- *Some tips towards cost reduction of the participant's network resilience processes: a) information sharing is an alternative way to increase efficiency; and b) contribution to the costs of upgrades might be required in the network fault area.*

5 Setting Reporting Procedures

Now that the broad outline of the reporting scheme has been drawn and the participants engaged in cooperation, it is time to begin mapping the details of the reporting scheme. This section discusses these details, beginning with reporting requirements, followed by prioritizing incidents, follow-up procedures, and media policies.

Figure 4: **Key Tasks in Setting The Reporting Procedures**


Identify the Need
Engage Cooperation
Set the Reporting Procedures
Manage
1. Reporting requirements
2. Prioritization mechanisms
3. Follow-up procedures
4. Media policies

5.1 Reporting Requirements

Deciding on the reporting requirements depends upon the area and purpose of the scheme, as well as such factors as the legal basis for the scheme, degree of willingness of reporting parties to submit sensitive data, experience of scheme managers and participants with the reports, and other factors. The following sections discuss the major issues that organizers must address, including report contents, types of reports and associated deadlines, and the channel for reporting.

5.1.1 Report Contents

Reported Fields

Deciding on the fields that should be involved in an incident report requires understanding the organizers' objectives, what they intend to do with the data, and the resources available to organizers and to reporting parties. Currently there are several standards available for incident reports, stemming mainly from a background in cybersecurity[6] and general incident handling[7]. In addition to that, a number of practices have crystallized in the network faults area, too. Though there are differences across areas of operation and the scheme's specific function, our research has revealed broad consensus on the items that are typically reported:

- Contact information,
- Time and location of the incident,
- Status information,
- Incident description,
- Incident impact,
- Incident handling description.

Contact information. Contacts to the reporting party including the name of the contact person, postal address, phone, mobile phone, and e-mail. Reference to the reporting party may be kept brief if the scheme's contact list is well-known and up-to date.

Time and location of the incident. If known, the reporting party should inform about the time and location of the event/failure that triggered the incident. Information about time zone should be added if the scheme covers more zones or is likely to communicate with other time zones, esp. for CERTs.

Status information indicates the status of the incident and its effects, whether the incident or its effects are resolved, and what period for recovery.

Incident description should provide information on the kinds of equipment or applications that failed, the sites or network areas affected, and on the incident causes. In cybersecurity, it may also involve identification of other sites involved either as sources or targets. In cybersecurity, it is a widely shared practice to require hostnames and IP addresses to identify any sites involved. Detected or estimated incident causes are extremely important, especially in cybersecurity where the scheme's organizers are supposed to alert stakeholders or assist in responding to the incident. Incident description is most easily provided by a narrative; in addition to that, the scheme may also use a set of categorized variables.

> ***NORS [USA],*** *a telco network outage reporting system, is using an open narrative describing "the sequence of events leading up to the incident, the steps taken to try and resolve the incident once it had occurred, and the action(s) that finally resolved the incident." On top of that, it also introduced the following variables to identify the incident's causes:*
>
> - *Direct Cause, or the immediate event that resulted in an outage;*
> - *Root Cause, i.e. the key problem which once identified and corrected will prevent the same or a similar problem from recurring;*

[6] CIP-008-2, ISO/IEC TR 18044:2004, ITIL Incident Management, NIST SP 800-61[rev1]

[7] ICS 201 and ICS 209.

- *Contributing Factors.*

The variables use the following range of possible cases: Cable damage, Design fault (Firmware /Hardware /Software), Environment (External /Internal), Hardware failure, Power failure, Procedural fault (Service Provider /System Vendor /Other Vendor), Simplex condition, Spare capacity failure, Traffic or system overload, Other or insufficient data or unknown. Furthermore, special variables are added to indicate whether, and to which extent was the outage caused by:

- *Lack of diversity in network design;*
- *Malicious activity.*[8]

Incident impact assessment is crucial for deciding upon follow-up, be it in emergency response or rectification mode. The variables usually eligible to measure impact of an incident are the list of network components affected; services or applications unavailable; special services such as emergency calls unavailable; customers and geographic area(s) affected by the outage. It is also possible to introduce a variable that would summarize economic social and economic impacts for the reporting party or for broader society.

Incident handling description. Finally, the report should contain a summary of the actions taken to remove the failure and possibly also to prevent its recurrence. As an attachment, this field may contain the lists of third parties contacted, documentation including forensic evidence, or in cybersecurity log files of actions taken by the reporting party.
The reporting format that a scheme would be using then would represent a specific combination of most or all of the abovementioned fields.

> ***FICORA [Finland]:*** *"In a notification to FICORA on a fault or disturbance in a communications network or communications service the telecommunications operator shall, where possible, give an account of the reasons for the fault or disturbance. The operator shall also submit information about the number of subscribers whose communications service was affected, other harmful consequences caused by the fault or disturbance and the repair time. The operator shall also inform about the measures it has taken or is going to take to repair the fault or disturbance in order to prevent such faults or disturbances or the harmful consequences."*

- *Depending on the scheme's objectives, a list of reportable information must be prepared which includs: contact information; time and location of the incident; status information; incident description; incident impact; and incident handling description.*

Standardization and Automation

The next question, directly following that of which information has to be submitted by the reporting parties, is whether the report should stick to strict formatting. As a means of formalizing and standardizing the report, the organizing authorities may use one or more of the following:

[8] Network Outage Reporting System User Manual, Version 6 (April 2009), http://www.fcc.gov/pshs/outage/nors_manual.pdf

- Questionnaires and forms,
- Pre-defined categories for variables,
- Web forms with pre-defined answers.

Standardized data input enables, on the one hand, sophisticated statistical analyses (see section 6.2), and on the other hand, a number of specific follow-up procedures. Several respondents in our research expressed the opinion that the larger the volume of reports submitted the greater the benefit of formalization and automation.

Categorization enables prioritization. If the number of reports submitted is likely to be high, it might exceed the capacity of human reviewers to assess each report individually. For these cases, the report should contain a categorized variable (most likely, one of the incident impact variables) that would attract the attention triggering a follow-up. (On prioritization, see section 5.2.)

Standardization enables automated processing. Similarly, if reaction to incidents requires immediate processing of a considerable volume of reports, especially triggering alerts or distributing information on an incident, standardized format will probably become necessary. In the cybersecurity area, many CERTs use machine-readable formats to automatically collect and distribute data on incidents on a daily or weekly basis. A corresponding software tool may be capable of working with several formats simultaneously. In any scheme with emergency response aspect, automated alerts may be sent out to stakeholders in reaction to reports containing critical levels of a certain variable.

> ***CERT-FI [Finland]*** *is running an automated reporting tool which works as "a collection of simple, but efficient, scripts. […] The underlying engine […] is responsible for fetching, categorizing, sorting, and formatting the reported incidents according to predefined templates. The engine also takes care of compiling the daily reports and emailing them out at predefined times to addresses found in our contact list. Each data source is attached to the framework through a tailor-made plug-in. […] Autoreporter is able to handle sources where data is either pushed (e.g., receiving data by email) or pulled (e.g., fetching the data from an external web server).*[9]

> ***MIMER/GLU [Sweden]*** *MIMER enables automated alerts in response to the messages submitted. Messages are handled in a uniform manner and the format used is XML.*

Standardization saves resources. Many operators are using automated network management tools on their networks. Standardization makes it possible to install interfaces that tune the inner reporting procedures of service providers with those of the public reporting scheme, thus allowing the operators to save resources.

On the other hand, we should say that standardization not only brings advantages. A number of respondents mentioned that standardization and formalization discourage the scheme's constituency from reporting. That is not only so because the reporting parties may feel overburdened by the reporting requirements, but also because standardization invites formalist attitudes:

[9] Thomas Grenmann of CERT.FI at http://www.cert.org/csirts/national/best_practices/2009/Autoreporter.pdf, p.2.

> ***[Government Authority]:*** *Follows the maxim that it is better to have the operators "think while reporting" rather than blindly follow a procedure.*

For that reason, some organizers avoid strict requirements and stimulate spontaneous reporting instead. This approach might be particularly suitable for schemes focusing on emergency response or for the schemes processing lower numbers of reports. If possible, it is also advantageous to apply lower requirements on new entrants who are only learning to participate in the scheme.

In any case, even if the reporting structure is not standardized, it doesn't mean that the reporting parties will not need the organizers' assistance in compiling the reports. Our respondents particularly mentioned informal discussions of the scheme's purpose and functioning with the constituency, reporting guidelines published on the web site, and follow-ups and clarifications on the reports submitted.

> ***[Regulator]:*** *"The experience is, the more informal the format, the more reports one gets." Therefore, the authority prefers not to overstretch formal requirements on the reporting parties. Based upon their first reporting, one can educate them on the desired format and suggest improvements for the next reports.*
>
> ***BSI [Germany]:*** *A list of "guidance questions" covering what should be reported is provided to the constituency.*

- *Pros and cons of reporting formats should be balanced when making a decision, especially on the benefits of flexibility vs. standardization.*
- *Over-formalization should be avoided: emergency response and low number of reports may not require formalization, while flexible formats can allow the easier sharing of whatever information the reporting party deems relevant.*
- *If a large number of reports is expected or if statistical analyses are planned the reporting format should be standardized. Use of categorized variables is recommended when it comes to incident prioritization.*
- *Automated tools must be used for large volumes of post-processed reports (emergency alerts or periodic information distribution).*
- *Assistance to the reporting parties should be offered: guidelines must be issued and requirements in informal communication must be clarified.*

5.1.2 Reports and Reporting Deadlines

The next thing the scheme's organizers will have to decide is the timing in which they would like to receive the reports (i.e. deadlines). Our research indicates that there are different kinds of reports for which different deadline policies are applicable:

- Initial report,
- Update report(s),

- Concluding report, and
- Periodical summary report.

Not all the schemes will use all the kinds of reports. The specific combination of reports and deadlines will depend on the reporting area, the kind of organizing entity, and the scheme's purpose.

Initial report. The initial report serves as notification that an incident has occurred, and should be submitted shortly after the fact. Initial reports are likely to be required in most schemes: they are essential if the scheme has an emergency response or rectification function, but also for alerting the constituency of failure-prevention schemes. As the main function of an initial report is a timely alert, the organizing authorities are sometimes less demanding in terms of formatting or completeness of the reports submitted.

In defining the deadline for an initial report to be submitted, many schemes can do with a general formulation "as soon as possible", or "as soon as discovered". In emergency response, the organizers may need to particularly cultivate the constituency's sense for urgency of timely reporting. In some schemes the organizers were able to set formal deadlines, usually around 1–2 hours, where a human factor is involved in reporting, or even less where the reporting is automated.

> ***MIMER/GLU [Sweden],*** *MIMER is working with an automatic format tuned with the reporting parties' Network Operation Centres. The technical design criterion is that a receiver will receive a message/report within a maximum of 5 minutes from the decision to report or update an outage information. There are several telecom operators that in normal circumstances (i.e. not during very large or severe disruptions) will have the messages produced and sent automatically.*
>
> ***FICORA [Finland]*** *proposes, in its draft regulation, network outages to be reported within 1 hour for the most serious incidents.*
>
> ***OFTA [Hong Kong]*** *decreed that for cable (backbone) outages, reports should be submitted within 2 hours from the confirmation of the outage or within 4 hours from the happening of the outage, whichever is earlier. For significant internet service outages within business hours (8:30AM – 1:00 AM) reports should be submitted within 1 hour from occurrence, else by the beginning of the business hours.*[10]

Update report(s). If the initial report is submitted as soon as possible, it is most likely that the incident information will be changing over time: the impact will escalate or decrease, new causes will be discovered or actions taken to fix the problem. Eventually the incident will be solved at some point of time. Depending on the purpose of the scheme, the organizers may wish to be updated on these changes with update reports, which may be filed in regular intervals, upon request from the scheme's organizers, or in reaction to events such as changing the incident priority, closing the incident or a new incident management call on the communication bridge.

[10] Office of the Telecommunications Authority: Guidelines for Cable-based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages, Issue 2 (January 2008), pp. 6,8,13.

In schemes with a large number of reports or with (partially) automated data processing it is recommended to assign to each incident a unique ID number for the purposes of tracking concrete cases and updating their status. It should be also said that not all schemes are using formal update reports; some prefer ad hoc updates with the reporting parties. More on the functions of updates in follow-up procedures will be said in section 5.3.1.

Concluding report. Most schemes run by bodies with a regulatory function do require an ex-post report as the service provider's statement on the incident. Some rectification-focused schemes may be limited to concluding reports only, but mostly the report will follow up on initial and/or update reports. The concluding report should contain full information in all reporting files, including analysis of the causes, and a summary of measures taken to remove the problem and prevent its re-occurrence in the future. Some of this information may only be available ex post, and also the reporting parties are more likely to assign human resources to detailed reporting after an incident has been solved than during the incident response itself. Concluding report is usually requested within days to weeks from the incident; sometimes the service providers are obliged to submit a draft within several days and the final version later on. The concluding report may serve as a basis of ex-post analysis of individual incidents, as described in section 6.1 below.

> ***NORS [USA]*** *expects first notification within 120 minutes from the incident, an Initial Report [draft concluding report] within 72 hours, and Final Communications Outage Report within 30 days from the incident.11*
>
> ***NPT [Norway]*** *works with a threefold structure comprising the first report, optional updates, and an optional post incident report. The first report is more of a headline-level notice to the regulator, containing basic characteristics of the incident and estimation of consequences based on the information available immediately after the event. The regulator may request more information especially on sensitive incidents, or the operators may send updates spontaneously. The regulator may request a post-incident report containing detailed information; such reports are submitted after the incident has been solved.*
>
> ***FICORA [Finland]:*** *The planned regulation requests first draft report within 1 hour from an incident, followed by regular updates (including special statement on reason why the outage hasn't been removed yet if the outage lasts longer than 3 hours), and a final detailed report within one week. "The first draft reports contain mainly information on the impact to the different telecom services (how many users are affected, what is the geographical area in question) and expected time when the disruption is over. The detailed reports include additional information, […] e.g. the original reasons behind the incident (e.g. stormy weather), the failed component in the network (e.g. DSLAM), description of how the incident was recognized (e.g. through network management system), description [of] what steps were taken to fix the problem, what was the time period of the service break, what kind of measures will the telecom operator take to prevent the incident from happening again."*

Periodical summary report. Finally for statistical purposes, information can be submitted in regular intervals – e.g., daily, weekly, monthly, quarterly or annually. Obviously, periodical reports can stand separately from real-time reporting: they would arrive regularly irrespective of the priority or volume

[11] Code of Federal Regulations, Title 47, Volume 1, Part 4, Sec. 4.5-4.9.

of reported incidents; they may report incidents that have not been reported individually; they may contain summary information but no details on individual incidents;

- *The types of reports and reporting timeframes must be taken into account: a) initial report, b) updates report, c) concluding report; and d) a periodical summary report.*
- *The initial report should be filed as soon as possible; awareness of the need for timely reporting must be promoted.*
- *A unique incident ID must be used for managing larger volumes of updating reports.*
- *Most detailed information must be quoted in a concluding report; this information might be used for follow-up analyses.*

5.1.3 The Reporting Channel

The final question to settle in the reporting requirements proper is the channel(s) that the scheme will use for reporting. The standard array of means available for that includes:

- Phone,
- SMS,
- E-mail,
- Web-based forms, and
- Machine readable messages.

Whichever channels are used for reporting need to be publicized among the constituency: the contact persons, phone numbers, email addresses, electronic interfaces, and finally reporting websites should be known and available to anybody responsible for submitting reports. For sophisticated platforms, such as web-based tools or machine readable messages (XML and others), it might be useful to compile a user handbook for the reporting parties. In terms of choosing the channel, there is no single good practice but a few suggestions have crystallized:

- For a quick alert or an initial report, the organizers mostly welcome information submitted through any channel. Keeping alternative reporting channels strengthens resilience of the scheme and increases chances of timely reporting.
- For emergency response, secure and resilient voice bridges offer the means of both reporting and coordinating the reaction.
- Machine readable messages (XML and others) and web interfaces are suitable for highly standardized reporting procedures, especially if automated data processing is involved.

Respondents from among service providers, vendors and scheme organizers cited the value of a single point of contact for reporting – the function known as *triage* in cybersecurity area. Having a single point of contact allows the reporting party to focus on solving the problem, because once an incident is reported, the scheme's staff then ensures information distribution and cooperation both within and without the sector, as described in section 5.3. Without a single point of contact, the reporting party must notify all customers and affected third parties of an incident directly, which may require a lot of resources. If legal or other concerns do not allow a reporting party to pass all information through a single point of contact, the organizing authority may at least mediate in making arrangements at lower levels and map those arrangements to enable a full understanding of the arrangements:

> ***MinEcon [The Netherlands]:*** *The Dutch Ministry of Economic Affairs is mapping bilateral business continuity arrangements, and it also is developing a template for bilateral agreements between the service providers and regional emergency response authorities. Having a centrally monitored and arranged map of agreements is part of the Ministry's CIP function, but it also assists operators who do not have the resources to negotiate at regional level. In addition to that, it assists the national operators by coordinating with regional authorities to prevent that the operators have to negotiate with each of all the regional authorities separately.*

- *The selected reporting channels must be widely publicized among the constituency.*
- *A secure and resilient voice bridge may be considered as a tool for emergency response. Other options are still valid: phone, SMS, email, web-based forms and other options.*
- *Quick alerts should be invited through any channel; alternative channels for emergency reporting must be kept.*
- *Machine-readable messages and/or web-based forms are recommended as regards the standardized and automated reporting.*
- *The scheme must be introduced as the single point of contact for reporting incidents within the eCommunications sector.*
- *The reporting parties must be supported in developing standardized and systematic arrangements for cooperation and information distribution.*

5.2 Prioritizing Incidents

Incidents need to be assigned a priority so that an appropriate follow-up action can be taken. Apart from that, prioritization may be used in order to communicate with stakeholders (alerts in cybersecurity often contain incident class) and to identify the proper respondent in case of emergencies (local/regional/national incident). There are three means that may be used to prioritize incident:

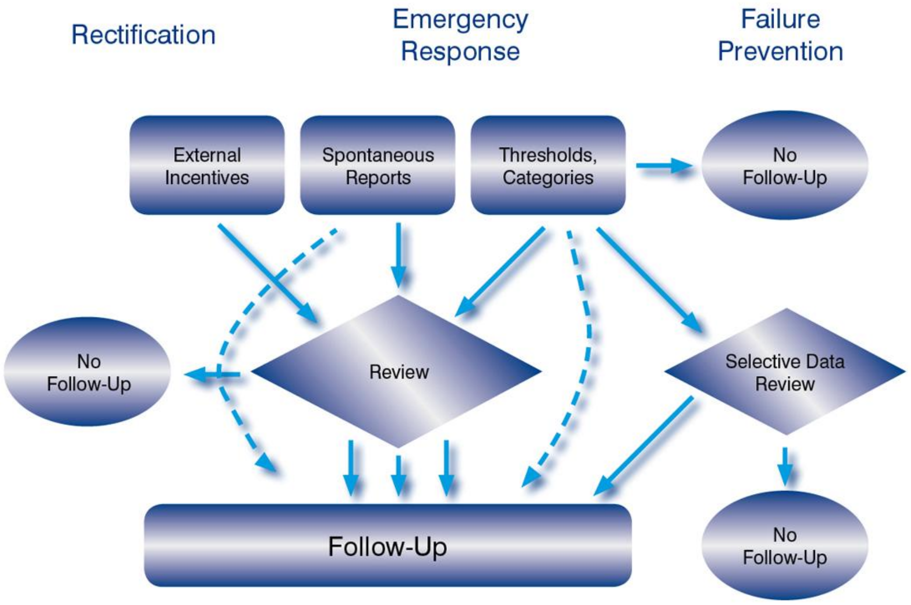
1. Reporting thresholds,
2. Reporting categories,
3. Human actor review.

In a way, the first step to prioritize an incident is taken when the reporting party decides to submit a report. In addition to that, many reporting templates contain categories that can be directly used for automatic prioritization. For instance if there are categories of the number of customers or area affected, these may be converted into priority classes as well. Finally, the submitted reports may be reviewed by a human actor and classified ad hoc.

From our research it results quite unequivocally that in order to decide on a follow-up action, review of incident reports and prioritization by a human reviewer is necessary. The reviewer may label the incident with pre-defined categories, or may simply assess its severity and decide on the appropriate follow-up.

Most schemes combine pre-defined thresholds and in-built reporting categories with a human review, thus optimizing the usage of human resources with respect to the scheme's priorities. Only in exceptional cases, e.g. where data is collected exclusively for the purpose of assembling ex-post statistics and no direct follow-up is expected, it is possible to skip the human element altogether. In the following paragraphs, we will present specific combinations of prioritization means examined by scheme purpose.

Figure 5: Prioritization Procedures in Incident Reporting



In emergency response schemes, the reporting parties are encouraged to spontaneously report outages that in their opinion require a follow-up. That might actually be a sufficient prioritization in itself; therefore in some schemes a reaction is triggered by any report coming in. In the majority of schemes, the organizers still wish to review the incoming reports and decide on their importance and the most appropriate follow-up. For the purposes of reviewing reports and managing the follow-up, the schemes with emergency response focus will probably need to establish a 24/7 service.

> ***ComReg [Ireland]*** *opens a communication bridge as a means of crisis management upon request from a reporting party [i.e., an operator].*

> ***MELANI [Switzerland]*** *maintains a 24/7 contact centre where members of the reporting scheme can report incidents. Based on the first input and possibly after discussion with the reporting party, a MELANI analyst on duty reviews the information available and assesses seriousness of the incident and assigns a category to it. The impact, direct or indirect, on MELANI members has priority over the impact on non-members. Finally according to the category, the analyst would decide whether to open the incident and what kind of stakeholders to notify.*

As said above, in rectification-focused schemes, the report may come either spontaneously from the reporting party, or upon request from the regulatory authority, after it learns about the incident from other sources, such as the media or user complaints. In both cases, the organizers need to consider severity of the incident and further actions to be taken.

> ***[Regulator]*** *"Incidents having a large impact on the telecommunication network are dealt with first hand, however, these are rather scarce. […] Cases of larger impact as well as cases with media coverage are those with highest priority."*

In failure-prevention schemes with an emergency response or rectification element the issue of prioritization becomes vital. These schemes sometimes invite a great number of incident reports to evaluate ex post. A small number of the reported incidents, however, requires an immediate reaction under either rectification or emergency response mode. Distinguishing the two kinds is essential to these schemes.

One possible means of overcoming this issue is to categorize according to the incident's seriousness. In the moment that the reporting party submits a report, the incident already is prioritized by the category and the organizers may react correspondingly. The number of categories varies; in our research no scheme would use more than five categories, while more common results were two to four. The criteria used are tuned to the scheme's purpose and would approximate the indicators that we already discussed for thresholds: request for assistance, impact on critical infrastructure or on other significant social and political interests and, most often, impact on consumers. The topmost category is usually the one that also requires earliest reporting, because the scheme organizers might need to organize an emergency response, or intervention for the purpose of urgent rectification.

> ***FICORA [Finland]*** *is currently drafting a new regulation, which prioritizes the faults and disruptions in telecom services and networks to 4 different severity classes (A, B, C and D). The classification criteria are based on the number of customers or the area affected [see section 3.3.3] The proposal suggests that the first report for faults and disruptions of severity class A would have to be delivered to FICORA within 1 hour; for severity class B within 12 hours; for severity class C within a week; for severity class D, only statistical information would be collected periodically.*

The other means, often used in parallel with the former one is to perform an independent data review looking for unusual patterns that may indicate a serious threat. The human reviewer may re-prioritize seemingly minor incidents as serious. This technique is particularly frequent in the cybersecurity area.

> ***[Reporting Scheme Manager]:*** *'A trivial incident, if repeated many times without an apparent reason, may be a signal of a possible threat to the national critical infrastructure. Our role is to spot those patterns.''*

- *A prioritization scale should be developed so that: a) an appropriate follow-up action can be taken, b) accurate information can be communicated with stakeholders (alerts in cybersecurity often contain incident class); and c) the proper respondents can be contacted.*
- *There are three means that may be used to prioritize incidents: reporting thresholds, reporting categories, and human actor review. Human review might be used to prioritize incidents in any scheme that requires follow-up action. Schemes combining failure prevention with another purpose usually need to combine human review with thresholds and in-built categorization.*
- *For emergency response, a 24/7 service should be maintained.*
- *If in-built categorization is used, differentiated deadlines for reporting should be considered. The most severe incidents must be reported in the shortest time.*
- *Data review in cybersecurity or in schemes with large volumes of reports must be performed.*

5.3 Follow-Up Procedures

5.3.1 Information Update

Upon receiving the initial report and assigning a priority to it, the organizing authority may decide to complete information either with the reporting party, or from other sources. Continuous updating becomes essential in emergency response-focused schemes, but also other types of reporting usually make some use of these procedures.

The widely shared good practice for instant updating with the reporting party is an informal follow-up, usually by a phone call, SMS, or email. Using contacts details submitted with the report, regularly updated contact lists, or their own trusted personal contacts, the organizers would reach the reporting party and request any missing information or informally consult the follow-up. For rectification purposes, or where the reporting parties are reluctant to submit full information, the briefing may be of a more formal kind.

> ***[Regulator]*** *"As soon as the regulator gets to know about an incident (be it by the provider, the media or another source) a briefing is required."*
>
> ***[Network Operator]:*** *If the operator is not submitting enough information or not reacting properly, the regulator can order a local audit of its network.*

The scheme organizers should be in position to get in touch with public CIP or emergency response agencies in real time and add information if the incident has a wider context (e.g., a power outage, fire, natural disaster etc.). They may also facilitate exchange of information among the organizations affected by the incident. In any case, as long as an incident is open, there should be a possibility to adjust its priority and update the information available.

> ***MELANI [Switzerland]:*** *Upon opening an incident communication bridge, the reporting party is invited to add input (log files, attachments, and other information). The public crisis management institutions may contribute with general information on the emergency, with analysis, alerts or recommendations. Also, other companies involved in the incident may submit information. The status and classification of the incident would be updated or changed according to the new information and in agreement with the information owner.*

- *Follow-up procedures must be in place so as to ensure information is updated and completed.*
- *In emergency response schemes, the incident information and status should continuously be updated until the incident is closed.*
- *Informal follow-up calls might be used so as to complete the information with the reporting parties.*
- *Additional information might be drawn from CIP and emergency response sources in case of a cross sector incident.*
- *Real-time information sharing among the afflicted parties must be invited.*

5.3.2 Coordination and Information Distribution

Based on the incident priority and possible updates to its status, the scheme organizers may need to extend notifications and to offer cooperation in a number of directions:

- To other participants of the scheme,
- To stakeholders within the sector,
- To CERTs,
- To regulators and authorities in other sectors affected by an incident,
- To emergency services,
- To other public authorities with emergency response or CIP capacity,
- To eCommunications regulator,
- To the media, etc.

The type and amount of information distributed, the addressees, etc. of course depend on the purpose and area of reporting, as on many other circumstances. Information distribution duties are particularly strong in emergency-response focused schemes. But also other schemes may need to forward information about incidents, following legal obligations in emergencies or obligations stemming from national crisis management plans. The schemes' staff must also consider which information they are not authorized to reveal due to the norms protecting privacy or business competition, and to individual non-disclosure agreements. Scheme organizers should be aware of their duties and train the staff correspondingly; the lists of authorities to notify in select cases and up-to-date contact lists should be part of operating procedures.

- *Obligations stemming from legal norms or national crisis management plans should be monitored.*
- *Contact lists should be kept up to date.*

In the following paragraphs, we will discuss three main areas where communication and coordination efforts are likely to follow upon a report: cooperation with the eCommunications regulator, cooperation with emergency responding agencies, and information distribution within the scheme.

Cooperation with Telecommunications Regulator

Close cooperation with the regulator is a possible, but not always necessary feature of a reporting scheme. Obviously in the schemes that are part of the regulatory loop (rectification and some of the failure-prevention schemes), the eCommunications regulator is the entity that receives the reports. It evaluates the statistical data, follows on individual incidents with the operators if necessary (see sections 6.1 and 6.2 on this), and adjusts its regulatory policies correspondingly.

> ***FICORA [Finland]:*** *"The incident reporting is a good tool for FICORA for understanding the actual quality, capacity, vulnerability and resilience of the telecommunications services in Finland. FICORA can use the gained results to focus the regulation topics to the most vulnerable parts (in incident prevention point of view) of the telecom operator's functionality."*

On the other hand, several respondents engaged in emergency response reporting emphasized that the regulatory function should stay out of the scheme. If the reporting parties assume that the reports would have consequences in terms of regulatory decisions or sanctions, they might not report as quickly, as often, or in as much detail as needed. That could have fatal consequences for the scheme's efficiency. Even if located inside one organization, the regulatory and emergency reporting functions may be separated to the benefit of the reporting scheme. That concerns both cybersecurity and network faults area.

> ***MIMER/GLU [Sweden]:*** *MIMER is coordinated and co-financed by the regulator (PTS) but focuses exclusively on helping to handle a possible crisis. The information submitted is to be used to understand the situation regarding ongoing disturbances and for the purpose of crisis management. An agreement has been made that the information is not to be stored or used for other purposes; for instance, it cannot be used to statistically analyze the occurrence of disturbances on different telecom operators' services over time. The regulatory purposes stay out of the scope of the project: the operators report voluntarily, are the owners of the data submitted, and can stop participating if they wish to. The operators have to file a follow-up report on serious incidents on their networks to the regulator, but that is not handled in MIMER.*

- *The regulatory function should not interfere with the reporting scheme's purpose: Either reporting is integrated into established and accepted regulatory practices; Or it is separated from the regulatory loop, especially for emergency reporting.*

Cooperation in Emergency Response

Coordination and communication during emergency situations is a very important role of most reporting schemes. There are three main functions that the scheme's organizers may be asked to perform:

1. To identify the incident owner;
2. To identify the emergency response level and relevant stakeholders;
3. To establish and maintain a communications channel.

In many cases an incident owner can be simply assumed to be the reporting party, but in other cases the reporting scheme's staff might need to intervene. For failures that result from interconnection of eCommunication networks (e.g., DDoS attacks), the scheme's staff needs to analyze the situation and decide whether there will be multiple owners or a single one. If an incident is not reported by the owner but by an affected party, the scheme organizers might need to investigate its causes and/or owners. Further intervention might be necessary if the incident owners are reluctant to accept their responsibility.

> ***NPT [Norway]:*** *In case of an incident involving physical infrastructure, NPT may assist in identifying the infrastructure owners.*

Another task to be carried out, simultaneously or even prior to identifying the incident owner is to identify the responding agencies that should be notified. The entities typically involved are

- National crisis coordination centre,
- Regional or local crisis coordination centres,
- Sector crisis coordination centres,
- Emergency services (fire, ambulance and other health services, police, civil protection, army), and
- CERTs for cybersecurity incidents.

The most effective way to ensure fulfilment of this function is to plan for it. The best practice here is for the reporting scheme to integrate into a national emergency response plan, whether sector specific, or general. Among other things, the plan would specify responsibilities, points of contact, and communication channels in particular kinds of emergencies. The plan not only clarifies duties but also reduces multiple reporting in introducing a single point of contact (a crisis coordination centre) wherefrom the information would be further distributed.

> ***UP KRITIS [Germany]:*** *The national Implementation Plan of Critical Infrastructures ("Umsetzungsplan Kritische Infrastrukturen", UP KRITIS), focusing on IT-security issues, identified communication as the key measure to ensure prevention, response and resiliency in*

CIIP. According to the plan, companies will be in touch with sector-specific contact centres (Single Points of Contact, SPOCs) which in turn will mediate communication with the national IT crisis coordination centre (BSI IT Situation Centre). The public-private partnership around UP KRITIS has outlined and is elaborating communication structures, procedures, and platforms to be used for detecting incidents and responding to them.[12]

CONOPS [UK]: *For emergencies, the British National Emergency Alert for Telecommunications (NEAT) is connected to the national emergency response scheme known as "Concept of Operations" (CONOPS). Within CONOPS, incidents are classified according to seriousness and geographic scope (national Level 1 to 3 + local); for each class of incidents, there is an agency (the Cabinet Office, a government department, the police) responsible for establishing and managing the crisis coordination centre.*[13]

If there is no such plan available, the scheme managers will have to make decisions on an ad hoc basis. According to the level of incident (local/regional/national), and its possible impacts at various sectors the responders will need to be identified and contacted. Even there, preparation is essential for success: without a contact list and emergency communication guidelines. Several principles followed in national crisis planning seem particularly recommendable:

- **Subsidiarity.** Crisis management should be as close to the level of the incident as possible; mediation by central agencies should be introduced only where functional.
- **Distribution economy.** Whenever possible, information should be distributed through single points of contact. For instance, to reach stakeholders in other sectors, that sector's CERT or crisis management room should be contacted.
- **Staying up to date.** Contact lists need to be updated regularly in order to support the emergency communication needs.
- **Practice.** Holding preparedness exercises can help to ensure that all parties are ready and able to coordinate and cooperate when needed.

Finally the scheme's staff may need to open and manage a channel that will be used for communication between emergency responders and eCommunications sector. That might not always be necessary: if a single company is involved, the subsidiarity principle suggests that the crisis management centre communicates directly with the incident owner. But whenever the incident requires cooperation of several stakeholders (e.g. in offering assistance or material support, rerouting the traffic etc.) or distribution of information among all stakeholders, the scheme's role is irreplaceable.

[12] *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen* (September 2007) [http://www.bmi.bund.de/cln_144/SharedDocs/Downloads/DE/Broschueren/DE/2007/Kritis.html], *Early detection and Mitigation of IT Crises* (December 2008) [http://www.bmi.bund.de/cae/servlet/contentblob/560094/publicationFile/27813/kritis_2_eng.pdf]

[13] *Central Government Arrangements for Responding to an Emergency: Concept of Operations* (March 2005), http://www.cabinetoffice.gov.uk/media/132685/conops.pdf

Sometimes the reporting scheme will host a communication platform that would include external emergency responders as external stakeholders, in other cases the organizing authority will function as a broker between the telco sector and the public crisis management centres.

- *Incident responders must be identified by assessing the scope and impact of an incident.*
- *Emergency responders must be assisted by identifying the incident owner(s) in case of complex incidents.*
- *Integrate with the national emergency response plan.*
- *Emergency communication guidelines must be prepared, including an up-to-date contact list.*
- *In involving other bodies, the principles of subsidiarity and distribution economy must be followed.*
- *Cooperation and communication in emergency situations must be exercised.*
- *If required, communication between emergency responders and the eCommunications sector might be moderated.*

Information Distribution within the Scheme

Whether mediating information exchange with emergency responding agencies, or for the purposes of purely internal communication, the scheme organizers will need means to share and/or distribute information among the participants. Depending on the incident circumstances, the participants may be exclusively from among eCommunications operators, or may include also major customers from among CI providers and/or public emergency response authorities. Managing the audience is an important part of successful information distribution and it is advisable to assign resources to the task.

> ***MELANI [Switzerland]*** *is a CIIP emergency responding scheme currently comprising 74 companies. It has divided its constituency into segments organized by sector (Energy, Telecommunication, Finance, Transport, Health, Government, Industry…). It uses a secure extranet to post the incident information (including, e.g. log files and any follow-up information). The extranet also allows the analyst on duty to manage access to the information posted: "Usually information exchange happens between MELANI and one company, MELANI and a whole sector, or in certain cases, between MELANI and the whole closed constituency."*

During the research, we have encountered three kinds of means for distributing information among the constituency:

1. Communication bridge,
2. Direct alerts,

3. Indirect alerts.

A number of emergency response schemes is organized around a communication bridge that would be opened at request of a reporting party. The bridge may be purely voice, but it may also contain functionalities for sharing data, GPS-enabled maps, etc. Upon activation of the bridge, the scheme organizers would notify relevant stakeholders via agreed contact means (mobile, phone, email, SMS) and invite them to join the bridge. Communications bridges enhance flexibility of emergency response and increase possibilities of cooperation and coordination under unpredicted circumstances.

> ***NEAT [UK]:*** *In case a serious outage is reported, the National Emergency Alert for Telecommunications (NEAT) will organize a briefing with concerned network operators at a dedicated secure phone bridge. Relevant staff are requested to call that bridge. The organizers would use whichever way available to reach the people or companies concerned: phone, mobile, or text messages.*

In cases when the scheme organizers do not have the resources, or enough reason to run a communications platform[14], they may send direct alerts to participants that are concerned with the incident. That obviously requires an up-to-date list of contacts in eligible companies, and usually also a human reviewer that would select the addressees. In some cases, automatic tools can be used for prioritizing and forwarding directly the incident reports.

> ***MIMER/GLU [Sweden]*** *is using incident reports submitted in a unified XML format. A disturbance that is handled by the service provider's Network Operations Centre is handled in different ways depending on the telecom operator (automatically/semi automatically/manually). The system supports the following information distribution and applications:*
>
> - *Public information announced on each operator's web page on a map of network outages.*
> - *Information forwarded to the public emergency response. While MIMER/GLU itself does not prioritize incidents, the data format allows the public emergency response agencies to forward receipts of the reports and/or run their own analyses of incidents (algorithms for incident prioritizing and handling).*
> - *Internal processes of the telecom operator (optional). The operators may use the format for applications alerting their staff or making information on outages available internally. This has been especially valuable for the efficiency of customer support and communication with service organizations, suppliers, or major customers.*
> - *Information is also distributed within the national crisis management communication tool (NTCG functionality).*
>
> *There are three different messaging formats that telecom operators can send as part of the Message Function: one for disturbances; one for "Normal network coverage" sent to the*

[14] Examples of initiatives in this area include: ms3i (http://www.ms3i.eu/ms3i), WARPs (http://www.warp.gov.uk), SecNet-IE, CIWIN, ISE architecture (http://www.ise.gov/pages/eaf.aspx) and NEISAS.

handler of the emergency call centres; and one for disturbances sent to other (depending) telecom operators.

Indirect alerts are the most economic way of information distribution, most likely to be found in cybersecurity area, where CERTs are publishing updates on threats on their web pages, or distribute alerts through mailing lists.

- *Assign resources to managing information distribution following-up on an incident.*
- *For intensive cooperation, consider hosting communication bridges.*
- *For delivering addressed alerts, maintain up to date contact lists.*
- *Where applicable, consider automatic information distribution tools.*
- *For large constituencies, launch public alert sites and mailing lists.*

5.3.3 Assistance to The Participants

Finally, to offer assistance to the reporting parties is another process used in a follow-up to a submitted report. According to our research, the practices in cybersecurity and network failures areas differ quite substantially, due to both nature of the incidents and distribution of resources. Organizers of schemes focusing on network faults often told us that removing an incident was the responsibility of the operators, who should have all the resources necessary to do that. What the reporting scheme can do is mediate in soliciting help from third parties: prompt the operators to assist each other with re-routing or mobile resources (exchanges, base stations), or arrange support from public resources.

> ***MinEcon [The Netherlands]:*** *The Dutch Ministry of Economic Affairs does not intervene into the technical solution of an incident, but it offers various kinds of institutional support to the incident owners. If necessary, it engages in exploring possibilities for rerouting the traffic with other providers. It may ask power ministries (interior or defence) to send staff to assist at the incident location. It may suggest to the local authorities to pay attention to the operators' request for support. It may use the media or the state Emergency Communications Network to distribute information about an incident.*
>
> ***NEAT [UK]:*** *As mentioned above, the British NEAT system will host a communication bridge in follow up to a serious incident, where the participants will arrange any cooperation necessary to restore the service as soon as possible.*

In contrast to network faults area, the reporting schemes in cybersecurity involve consumers of IT services and many small service providers. Therefore the scheme's staff is more likely to possess know-how and resources to help.

They can distribute malware analysis or removal patches. They may intervene with ISPs whose network(s) host attackers and e.g. ask for, or enforce, shutdown of attacking servers. The scheme organizers – usually CERTs, GovCERTs etc. – may also offer technical consultations or, if their legal status allows, send technical staff to the premises of organizations affected by an incident.

***CERT/CC**, defines the following services that a CSIRT offers to its constituency during the Incident Handling stage:*

- *Incident analysis: identifying and documenting the extent of damage caused by an incident, the nature of and available response strategies to the incident. Incident analysis may include tracing attackers and collecting forensic evidence on their activity.*
- *Incident response on site: CSIRT staff analyzes the affected systems and conducts the repair and recovery of the systems.*
- *Incident response support provided via phone, email, fax, or documentation. This category covers technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies.*
- *Incident response coordination: When multiple parties are involved, the CSIRT notifies sites of their potential involvement (as victim or source of an attack), collects statistics about the number of sites involved, and facilitates information exchange and analysis.*[15]

- *In the network faults area, focus on mediating mutual support between stakeholders and assistance from third parties.*
- *In the cybersecurity area, develop capacities to offer assistance in incident handling: analysis, consultations, on-site help, etc.*

5.4 Media Policies

Incidents can affect large numbers of people, businesses and services, and they can have public safety ramifications. Therefore, they are potentially of interest to the wider public. The role of media in informing about incidents is essential, and media-related activities may pop up all along the operational cycle of a reporting scheme. Because most of these activities concentrate around follow-up to an incident, we choose to discuss this issue here. Our research suggests that there are four kinds of situations where the reporting scheme's staff is most likely to work with the media:

1. Collecting information about incidents;
2. Answering queries from the media;
3. Distributing information about incidents;
4. Raising awareness about threats.

Collecting information. Media are valuable additional sources of information about incidents. Where the service providers do not feel motivated to report, or are impeded from reporting by external factors, media may be the first to bring an outage to the attention of the scheme's organizers. Media attention may also signal social sensitivity of an outage. Monitoring media coverage thus becomes

[15] http://www.cert.org/csirts/services.html#reactive

important, especially in schemes with a rectification element, where the organizers may request the service provider to report about such incidents.

Answering queries. Many scheme organizers are approached by the media with queries about threats or particular incidents. While their public function obliges the organizers to inform, they also have to respect legal obligations for protecting privacy and business secrets. As argued in section 4.5.1 above, confidentiality is a major concern of the reporting parties, and indiscrete handling of the data might demolish the trust towards the scheme's staff. As a result, the media policies need to delicately balance multiple obligations, a task which mustn't be under-estimated. The respondents mostly recommended commenting generally on the type of incident, on its consequences for the public, vulnerabilities that people should be aware of, and other necessary details, while avoiding pointing fingers publicly at specific companies, or releasing specific company data about the incident. Issuing guidelines, training the staff appropriately and/or assigning the role of spokesperson are practical steps that may help in handling this issue.

> ***[Regulator]*** *"public relations experts are always involved, in order to ensure fast and competent response towards the media in case of requests."*

Distributing information. In certain cases, the scheme organizers need to actively counter rumours or panic, to inform a large audience about an event, a threat, or a progressing incident response, or to distribute other critical information. The organizers rarely have better means to do this than through the media. For this purpose, again, it is vital to cultivate know-how in dealing with the media – e.g., organizing press conferences, producing and distributing news releases, etc. In certain cases this role is assigned to special organizations within the government sector with which the scheme staff cooperates.

> ***[Government Ministry]:*** *"Where media can distribute information on the progress of incident response or actions to be taken by the public, the media co-ordinator which is close to/part of the crisis response team will cooperate with media. Also information from outside the crisis management teams / structure which is gathered by the media is used in decisions on the response actions."*
>
> ***FICORA [Finland]:*** *In the case of a small-scale DDoS attack in Finland shortly after the 2007 attack on Estonia, FICORA reacted with a press conference in order to prevent panic and inform the public appropriately.*

Raising awareness. Continuous awareness building belongs to regular operations especially in cybersecurity failure prevention – or in other words, in the CERT area. There the organizers need to educate the public about vulnerabilities and threats, and also about good practices how to avoid further incidents. Again, media are an important channel for doing that. Maintaining up-to-date and well structured web sites, regular contact with the media via news releases, seminars, newsletters, email alerts etc. belong to the best practices here.

> ***INTECO CERT [Spain]:*** *"A large number of media are subscribed to our advisories and alerts of our website so they are in contact with us. Sometimes the media contact us requesting more information or advice about security issues: alerts, advisories, etc. We believe in the importance of Web2.0, and especially RSS/XML applications in awareness raising activities."*

- *Reporting schemes will typically interact with the media under several circumstances: when media report about an incident; when they request comment from the authorities about incidents; when the authorities need to communicate with the public about an incident, and when organizers need to raise awareness about incidents or threats.*
- *Elaborate media policy and train/employ staff for answering media queries.*
- *Use media actively for distributing information about serious incidents or countering rumours and panic.*
- *Develop a long-term media strategy for continuous awareness raising.*

6 Managing Reporting Scheme

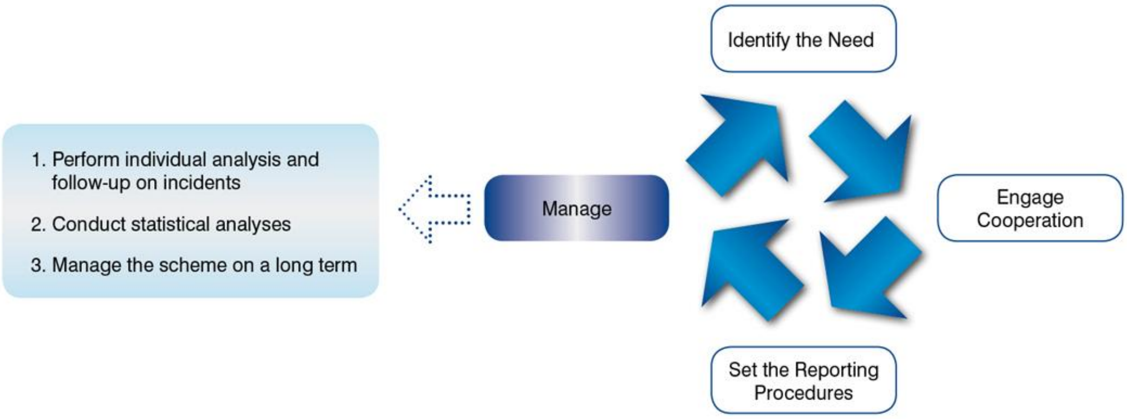
The previous three chapters have discussed how to identify an incident reporting need, how to engage cooperation and arrange concrete reporting procedures. Apart from these tasks, mostly located around the launch of the scheme, the scheme needs attention as it operates. On the one hand, incidents need to be monitored and evaluated in order to implement appropriate reactions: network topology upgrades, awareness raising, changes in cybersecurity or emergency response policies. On the other hand, the organizers need to manage the evolution of their scheme. Then it becomes important to collect feedback on the scheme's functioning and to plan improvements or extensions.

In this chapter, we will review three channels that may serve to monitor and manage the reporting scheme:

1. To analyze incidents individually and follow up with the incident owners;
2. To evaluate incidents statistically and draw lessons;
3. To manage long-term evolution of the scheme.

The practices quoted in this chapter should help in disseminating information to the constituency, requesting particular changes at the service provider's networks, collecting information on the scheme's functioning, and adjusting its structure as the nature of the challenge develops.

Figure 6: Key Tasks in Managing The Reporting Scheme


1. Perform individual analysis and follow-up on incidents
2. Conduct statistical analyses
3. Manage the scheme on a long term
Manage
Identify the Need
Engage Cooperation
Set the Reporting Procedures

6.1 Ex-Post Analysis of Individual Incidents

Ex-post analysis of incidents is a critical part of the incident reporting scheme’s responsibilities. There are several benefits to be drawn from the process:

- Educating the scheme's constituency,
- Making sure that the lessons are learned,
- Identifying and facing new challenges,
- Ensuring rectification of faults.

Many schemes, especially in failure prevention and rectification, request the reporting parties to submit a post-incident report stating not only the nature, duration, and impact of an incident, but also its causes and actions taken in order to restore the services and to prevent similar events in the future (see section 5.1.2 above).

For serious incidents, the scheme organizers may proceed towards ex-post assessment. The analyses may point to desirable improvements in reporting as against the experience during the case, and also look for better means to prevent failures in the future. In select cases, analyses may be commissioned externally.

> ***ComReg [Ireland]:*** *Upon closure of a communications bridge that was open during an incident, the expert group that would be mobilized to assist during incident response may decide to compile a report on the incident, or alternatively suggest commissioning such a report with a third party.*
>
> ***FICORA [Finland]:*** *"In case of critical faults or disruptions, FICORA may analyze in detail the reasons behind the incident, the telecom operator's actions and other issues around the incident. Also incident-specific meetings with telecom operators may be arranged."*

These analyses then may be used to educate the wider community of stakeholders about new threats and about the scheme's requirements and functioning. Reviews of major incidents experienced and lessons learned may avoid revealing sensitive company details, but still share broader concerns and advice. Case studies, comments, and alerts may appear:

- In newsletters or at websites,
- At seminars or workshops for specialists,
- At regular stakeholders' meetings,
- In one-to-one reviews with the service providers.

As already mentioned, in emergency response-focused schemes, some stakeholders might get concerned should their reports trigger a regulatory reaction. If the reporting parties are owners of the data submitted, they may even refuse to give authorization to the reports' usage for other purposes than immediate incident response. As trust is being built up, it becomes possible to discuss incidents informally in trusted expert groups or to disseminate anonymized information.

If reviewing the incident one-to-one with the operators, it is advisable that the organizing authority works in an atmosphere of trust and mutual profitability.

> ***[Operator]:*** *The company sees added value in follow-up analyses with the regulatory authorities. The authorities get a view how the company operates, and the company can demonstrate that it has solved the problem successfully.*

On the other hand, the scheme's organizers will be able to rely on the interest of service providers in maintaining business continuity. A number of respondents from both public and private sector asserted that most operators were learning the lessons from an incident quite spontaneously and it was enough for the organizing authority to supervise the process in post-incident reports or one-to-one talks.

> ***[Government Institution]*** *"[…] what normally happens is that operators and service providers are the first to update their preparedness measures, as they could be affected financially by any kinds of disruptions, so it is in their interest to be well prepared."*
>
> ***[Network Operator]:*** *"Breach of Customer SLA's is […] a driving force/incentive for network operators & ISPs in ensuring continuous network availability[;…] the ultimate punishment […] is loss of customer business."*
>
> ***[Network Operator]:*** *"Being out of service is the same as loosing income during the period of incident."*

Serious or novel incidents are likely to be brought to the attention of a Network Security Information Exchange (NSIE), too. NSIEs serve, among other things, as a platform for key players in the eCommunications sector to share information about the most serious incidents, assess their impact, and draw corresponding lessons.[16]

> ***NPT [Norway]:*** *For any incident that is new as a type, whether serious or not, the Norwegian Regulator NPT is likely to request a follow-up report from the operator analyzing the threat. NPT may compile a summary report.*

Finally, using the above investigations and reports, some regulators have the authority to require improvements, control the implementation, and impose sanctions if necessary. In case that the vulnerabilities discovered by a case review are not situated at an individual operator's network but at a shared location or function, the regulatory authority would probably wish to coordinate and induce necessary changes at individual operators' networks. The regulatory policies proper being beyond the scope of this report, let us only remark that scope and format of the measures used vary greatly according to the local legal framework and regulatory philosophy.

> ***Regulatory philosophies [General]:*** *Regulators in Finland and Norway prefer regular meetings with the operators to perform reviews of incidents and request upgrades on the operator's networks. The German system builds on the concept of a security plan that each operator is obliged to submit to the regulator. Following on an incident, a post-incident report may be required, followed, if the regulator opts so, by a mandatory upgrade of the security plan and/or inspections on the service provider's premises.*

- *Ex-post analysis is a crucial part of an incident reporting scheme. It helps in educating the scheme's constituency (learning from experience), identifying and evaluating threats, and ensuring rectification of problems.*
- *Use incidents as an opportunity to educate the reporting parties: via individual follow-up; and via alerts and exemplary lessons for newsletters, workshops and meetings.*

[16] See ENISA's Good Practice Guide: Network Security Information Exchanges, June 2009, http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide

6.2 Statistical Analysis across Incidents

Statistical overviews are the way to identify lessons from the large pool of data about incidents. These overviews can be very useful in identifying vulnerabilities and discovering longer-term trends in the evolution of threats, especially with the failure-prevention objective in view. However, our research has revealed that at present, they are far less common than the individual follow-ups. Several scheme organizers recognized value of statistical analyses and either plan to add longer-term analysis of incident trends, or expressed interest in doing so.

> ***CERT-FI [Finland]:*** *"The most interesting observations can be made by looking at the statistics over a longer period of time. […] In addition to looking at yearly trends and categories of incidents, we like to scale the total number of incidents against the number of existing broadband subscriptions. We reason that the number of incidents should correlate with the number of computers brought online."*[17]

There is a difference between the ways statistical updates may be used in cybersecurity and network faults areas. In cybersecurity, regular – especially daily – updates on attacks, as we know them from CERTs, can prove of direct relevance to the stakeholders. If the summaries enlist, e.g., the kinds of malware that caused incidents, they may serve as threat alert or an update on current status of threats. Obviously, these overviews in cybersecurity can only be produced with an automated tool.

In the network faults area, more in depth analysis seems necessary, usually released quarterly to annually. Our research pointed to several conditions that need to be in place in order to seek for trends and correlations in the data on causes of incidents, outage times, speed of recovery, etc.:

- Enough reports to analyze,
- Richness of data,
- Resources to perform analysis.

To increase the number of reports submitted to a level that enables valid statistical processing, it is possible to expand the scope of the reporting scheme, to lower thresholds, or simply to add data from other sources. In both cybersecurity and network faults areas, it is useful to consider using additional sources, too. Our respondents particularly recommended using honeypots and sensor networks that identify malware, botnet activity, spam, etc., and collecting data from automated network management software tools used by the service providers.

> ***INTECO CERT [Spain]:*** *In addition to the voluntary reports submitted by the service providers, INTECO CERT uses also end-user reports, surveys, periodic scanners, and data from honeypots and security sensor networks.*

To ensure data rich enough to allow statistical analyses, it seems necessary to work towards enriching the reporting formats and tuning them to the kind of analysis that is intended. For instance, the reporting format should eventually contain classification of the incident causes. The organizers should bear in mind that some information may only be available from ex-post reports.

[17] Thomas Grenmann of CERT.FI at http://www.cert.org/csirts/national/best_practices/2009/Autoreporter.pdf, p.2.

Finally, statistical procedures may require additional human resources to perform follow-up inquiries that would complete the data submitted, carry out in-depth analyses and write up reports. These may be internally within the organizing authorities, or commissioned externally (at the universities, partner organizations etc.). To support the data processing, it may be necessary to employ a special software tool, whether for real-time updates (daily reports) or for assembling, transforming and compiling the reports submitted.

Statistical analyses may be used for the same purposes as the individual follow-ups. Statistics gathered from various resources are often used as the basis for one-to-one talks with service providers; they allow comparisons and visualize vulnerabilities on particular networks.

> ***FICORA [Finland]:*** *"FICORA meets the main telecommunications operators on a yearly basis on the subject of last year's faults and disruptions in telecommunication services and networks. During these meetings FICORA presents some statistical information on the latest data received, e.g. what are the main reasons behind the faults and disruptions and what are the most vulnerable components in the networks."*

The statistical data are particularly suitable for identifying vulnerabilities at the national level and for drawing corresponding lessons. As with the individual follow-up analyses, the statistics represent value added to the scheme's constituency, thereby helping to demonstrate the scheme's relevance, build trust, and encourage voluntary cooperation. Once again, in publishing and discussing the statistics, the organizing authority has to pay attention not to compromise confidentiality of the received reports.

- *The use of statistical analysis of a large volume of reports might be considered as a way to identify lessons from the large pool of data about incidents.*
- *In the cybersecurity area, automatic summaries on attacks might be organized. In the network faults area, in-depth analyses released quarterly to yearly might be considered. An appropriate data collection framework should be established to support the incident analysis. Reporting format should be enriched so that more correlations may be performed.*
- *Analysis should be supported by enough resources; both human and technical.*

6.3 Long-Term Management

No reporting scheme should be perceived as the final product. Threats and challenges develop, and so do the needs of the public and the reporting parties themselves. Therefore, adjustments are a necessary part of the business of running an incident reporting scheme. On the one hand, the organizers should continuously try to tune and improve the scheme's performance within the selected area and purpose. On the other hand, they may need to consider broadening the scope and adding new functions to the standing scheme. We will address these two kinds of long-term management in separate subsections.

6.3.1 Scheme Improvement

This subsection will discuss means used for improving the scheme's performance within the already selected area or purpose. Ideas for improvements will appear while analyzing the incidents, whether via individual ex-post or a statistical examination. The other essential source of impulses is feedback from the reporting parties. The points of interest for the organizers are problems encountered with reporting, requests for support, and suggestions for the scheme's further development. The most recommendable practice is to ask for feedback regularly, whether in one-to-one consultations with service providers, or in regular meeting of stakeholders and/or expert groups.

> ***MELANI [Switzerland]*** *is an emergency response scheme run with a pool of select CI providers across various sectors. Depending on the sector, the organizers hold semi-annual sector-wide meetings of stakeholders in order to discuss lessons learned, but also to listen to the wishes of stakeholders and collect suggestions.*
>
> ***CERT-FI[Finland]*** *The Finnish national CERT organizes working group meetings four to five times a year that discuss new threats and other issues. The group involves representatives of major service providers, customers and some public institutions.*
>
> ***NPT [Norway]*** *holds yearly one-to-one evaluation meetings with the largest operators, which, on the one hand, evaluate the operators' networks and discuss incidents, and on the other hand collect their feedback.*

Communication with stakeholders is a presupposition of successful long-term steering also for other reasons. The organizing authority needs to educate the constituency on new requirements and new threats, and it also needs to maintain and increase commitment to the scheme's goals. Some authorities recommend informal follow-ups on reports, discussing improvements in both reporting standards and resiliency measures of the given reporting party; others hold seminars, workshops, conferences, or forums for discussion; yet others issue regular reports on activity and analyses for this purpose.

> ***[Regulator]:*** *"Build on trust, show the need [for reporting], provide feedback when reported, create and communicate added value […] for the reporter."*

During our research the respondents most frequently mentioned coverage of their respective schemes as subject to improvements. Thus the improvements might have concerned:

- Extending operation time,
- Enlarging the constituency,
- Increasing data volume.

The scheme's operation time may be extended from business hours or great emergencies to a 24/7 model. Including new sectors or smaller service providers may expand the constituency. Finally, the volume of data may increase upon lowering the reporting thresholds and/or refining the reporting template. With more and better data, more sophisticated analyses of threats and recommendation for avoiding them become available, which in turn may increase the value given back to the community.

> ***Theodore Puskas Foundation [Hungary]:*** *"National High-level Service for Communications and Informatics […] has been set up in 1995 to monitor and gather data regarding system breakdowns/availability in the field of telecommunication, but it was operating only for example during floods. Meanwhile, the scope of this service was widened, and nowadays this duty service operates […] 24/7, monitoring the system breakdowns of major Hungarian telecommunication providers, broadcasting companies, post services and network security issues."*

More often than not, significant broadening of coverage is connected with increasing codification of reporting duties and formalizing the requirements. Introducing legal obligations and sanctions has been recommended as a good practice by several respondents, but others mentioned that in emergency response schemes and those based on private-public partnership, this may not be always advisable. In any case, the organizers introducing additional obligations should keep in mind that new formal requirements usually need a time for tuning. After the new requirements are launched, the organizers might need to collect feedback, adjust the settings, or allocate more resources to handle the scheme's operations.

> ***BSI [Germany]*** *is in the process of codifying the obligations of the reporting parties. It expects that the number of submitted reports will rise after mandatory reporting will have been introduced and plans time for adjustments of both reporting template and data processing.*

> ***FICORA [Finland]:*** *Similarly FICORA says that it will need to keep an eye on the volume of reports submitted after new regulations will have been introduced. If necessary, they would consider using an automated tool for processing the reports.*

- *Feedback should be collected on a regular basis.*
- *Constituency must be trained and its commitment must be maintained.*
- *Scheme's coverage must be expanded and the value given back to the constituency must be increased.*
- *Reporting requirements must be formalized.*
- *Put aside time for tuning the scheme after introducing new requirements.*

6.3.2 Scheme Evolution

From a global point of view, it is desirable for any country to have as complete coverage of reporting functions and areas as possible. Therefore the moment may come in a reporting scheme's lifecycle to consider expanding beyond the original area and/or purpose of reporting. That is an important, but also sensitive step, because it involves adding new focuses to the activity of the organizing authority and possibly changing the business culture, legal status or function it originally came from. This subsection should help you to reflect on the background that your scheme comes from and on the challenges that might be connected with extending beyond its original boundaries. The reflections cluster around the scheme's organizing authority. Our research has identified several kinds of entities that organize reporting schemes:

- Telecommunications regulatory authorities,
- National / governmental CERTs,
- Authorities engaging in critical infrastructure protection,
- Other non-national CERTs.

With respect to the purpose of reporting, the table below summarizes the typical associations. Most likely, your own scheme will have begun in one of the fields marked by a cross: e.g., if you are a CIP Authority, then in emergency response but not in failure prevention or rectification. In addition to that, national and other CERTs are likely to operate in cybersecurity reporting area, whereas telco regulatory authorities will mainly cover the network faults area.

TABLE 1: Types of Institutions Hosting Incident Reporting Schemes

	Telco Regulatory Authority	National / GovCERT	CIP Authority	Other CERTs
Emergency response	**X**	**X**	**X**	**(X)**
Failure prevention	**X**	**X**	**–**	**(X)**
Rectification	**X**	**–**	**–**	**–**

Whenever a new purpose or area is added to the scheme, that means coping with limits imposed by the previous context. The possibilities, challenges and recommended practices will differ according to the status of the organizer.

In the CERT area, we can observe a tendency to promote existing CERTs to the role of national CERTs that would offer assistance in incidents of national significance and serve as official national points of contact for other national CERTs. It is particularly likely that the functional areas of national and governmental CERTs would merge, which seems to justify to speak of a national / governmental CERT type. It should be noted that promotion to a national / governmental level might require improvements to the CERT's legal status.

> ***CERT-LT [Lithuania]*** *started from a CERT hosted at the Communication Regulatory Authority (CERT-RRT, established in 2006). In 2008 government decided to promote it to a national CERT.*

CIP authorities are in a more complicated situation. Adding functions to the emergency response schemes that they are likely to run means extending the organizer's status into a new area as well. The research that we have conducted suggests that responsibilities of a CIP authority are easiest to coalesce with those of a national / governmental CERT. That means that CIP authorities are most likely to expand into emergency response and failure prevention in the cybersecurity area.

***BSI [Germany]:** The German Federal CIIP authority BSI (Bundesamt für Sicherheit in der Informationstechnik) is hosting also CERT-Bund, the Federal GovCERT, as its department.*

As we have remarked in section 5.3.2 above, emergency response functions may be difficult to appease with the regulatory ones. For that reason, we see CIP authorities as less likely to extend their status towards telco regulation, and their function towards assuming failure prevention and/or rectification responsibilities in the network faults area.

National /governmental CERTs can boost their emergency response and failure-prevention capacities by moving into critical infrastructure protection, or by assuming some kind of a regulatory role. Some CERTs have emerged as a grass-roots initiative of industry and are based on voluntary participation; in those cases introducing regulatory powers needs to be discussed with the constituency first. There is also the possibility to federate functions very loosely. For instance, the facilities already used by CERT (such as a 24/7 service, operations centre, etc.) may be also used for running another institution.

***Theodore Puskas Foundation [Hungary]** is running its own scheme in the cyber security area (CERT Hungary), but it also hosts the national communication network failure reporting scheme; the latter function has been commissioned by the national regulator (NHH). While both schemes are using the same infrastructure, the follow-up differs and is managed separately by CERT Hungary and the NHH. Although the two duty services are separated by function and staff, they cooperate on the basis of sharing security events related to IT security.*

Our research suggests that the regulatory authorities in telecommunications are best suited to federate functions. Indeed it is quite feasible to combine a failure-prevention scheme with alerts in cases of emergencies or high priority incidents, and with possible rectification-oriented follow-up. Some European regulatory authorities host national CERTs (e.g., RRT in Lithuania, FICORA in Finland), while others run emergency response schemes (e.g., PTS in Sweden, ComReg in Ireland).

This document is far from recommending boundless federation of functions within one scheme. Indeed some benefits can only be obtained from specialized schemes. For instance, an efficient emergency response scheme may be better kept separately from the regulatory loop; also mergers between the cybersecurity and the network faults areas within one scheme are rarely seen. In these cases, the telecommunications regulatory authority may consider simply hosting two different schemes.

***FICORA [Finland]:** The Finnish regulator runs a network faults prevention scheme with some emergency response aspects, and separately also CERT.FI.*

***MIMER/GLU [Sweden]:** The Swedish regulator PTS is coordinating an outage reporting scheme MIMER/GLU. The scheme is exclusively focused on helping to handle a possible crisis and is separated from the regulatory reporting loop.*

Evolution of incident reporting schemes is only part of the integration of CIIP policies at both national and European levels. As these efforts progress, the organizers of the reporting schemes will be looking towards necessary adjustments in the legal framework. Those would aim, on the one hand, at improving the scheme's legal status, the right to demand cooperation etc., and on the other hand, at harmonizing the incident reporting with other components of the national CIIP policies. Clashing jurisdictions or other obstacles to cooperation will have to be sought and removed. Indeed, many of the European schemes we have reviewed for this report are in the process of expanding and updating their respective legal basis, or have recently undergone such a process.

The road to better incident reporting passes through many crossroads, the most important of which we tried to outline in this section. There are as many ways of developing a national incident reporting system as there are business cultures, administrative traditions and legal arrangements. In some countries, incident reporting even isn't the primary means of ensuring failure prevention or rectification. In any case, as the eCommunications landscapes get more and more populated with reporting schemes, both the standing schemes and the host organizations will undergo changes. During this process, the organizers will need to think in a forward-looking manner and actively search the spaces for their scheme to evolve to.

- *Clashing jurisdictions or contradictory objectives or responsibilities that may undermine efforts to expand the scheme into new areas must always be taken under consideration. New responsibilities must always be complementary to the initial ones.*
- *If the purpose of reporting expands, expand the status of the organizing entity*[18]*.*
- *Consider running schemes separately if it benefits their functions.*
- *Support integration to the national CIIP policy with legal framework adjustments.*

[18] For example, promote a CERT with limited constituency to a national / governmental CERT; include CERT functions into the operations of a CIP authority; strengthen CIP or regulatory powers of a national CERT; or federate functions within a telco regulatory authority.

7 Conclusion

As Europe's countries, institutions, businesses, and societies become more and more dependent on information infrastructure, they must ensure the resilience of that infrastructure.

The European Commission noted in its communication on CIIP that there is inconsistency in the implementation of early warning systems, information sharing, and coordination for incident response. Incident reporting schemes are necessary to enable quick response and coordination by all institutions affected by network incidents and that must act to resolve the incidents. And these schemes also enable the longer-term prevention of similar incidents.

The inconsistent development of incident reporting schemes across the EU presents both a clear need, and a clear opportunity. It is a clear need, since those Member States with little incident reporting in place, or with insufficiently effective schemes, have a need to introduce or adapt their schemes. But it is also an opportunity, since the existence of several diverse schemes in various locations provides many examples of types of schemes, approaches, objectives, procedures, etc. It also provides a great deal of expertise from public authorities, private-sector participants, CERTs, and other participants and stakeholders, who have developed, managed and participated in such schemes. And it yields numerous good practices that can be analyzed and applied by others.

This report attempts to draw on the experiences that experts have with reporting schemes where they exist. It then attempts to provide a framework for analyzing the existing schemes and the needs that authorities may have, so that these authorities can adopt those good practices most relevant for their situation.

The development of national reporting schemes is an important objective in its own right, but it also enables some further developments, as well. One key possibility for further development includes international coordination.

In the Commission's communication on CIIP, the Commission not only emphasized the need for national reporting schemes, but it also emphasized the need for improved coordination and cooperation across Member States. As noted many times above, the communications networks, and the threats to them, are becoming more and more international. Furthermore, the expertise about threats, and how to prevent and respond to incidents, is distributed internationally. There is a great opportunity for Europe's experts to pool their expertise and to make substantial strides forward in increasing network resilience.

ENISA's role in facilitating this kind of cooperation and knowledge-sharing was emphasized and reinforced in recent EU statements, including the communication on CIIP, and now in the new reformed telecoms package. Based on its defined role, the agency continues to identify good practices and share them with stakeholders throughout the EU. The agency also continues to facilitate knowledge sharing through other means, including public events and support for public-private partnerships.

This report is but one example of the international cooperation described above, and ENISA's efforts to support it. The document attempts to consolidate the experiences across Europe with reporting schemes, and facilitate the sharing of expertise. Additionally, the process for preparing this document

– interviewing experts across the EU – revealed a great deal of interest in such sharing and cooperation. Experts from public and private sectors and beyond were motivated to share their experiences and recommendations.

Given the existence of motivated experts across the EU; diverse experiences to draw upon; increasing opportunities for cooperation; increasing development of public-private partnerships among stakeholders; ENISA's position as a facilitator; and the legal and policy support at Member State and EU level; there is a great deal of reason for optimism on several issues. First, national authorities should be able to implement effective incident reporting schemes. Also, national network resilience will increase as a result. International cooperation will be a facilitator of this development, as well as benefiting from it. These steps will play a useful part in the wider initiative to increase resilience of critical information infrastructure. And finally, these steps will play a useful part in the wider efforts to increase international cooperation among stakeholders in the efforts to increase network resilience.

8 Appendix A: Checklist of Tasks and Recommendations

Status	Task/Recommendation
Stage: Identifying The Need	
	Task: Examine the status quo
	Map the existing processes, procedures, institutions, and stakeholder interest in CIIP.
	Identify gaps that require a new reporting scheme.
	Avoid unnecessary duplicating or contradicting the existing efforts.
	Identify know-how and institutional foundations that your scheme may build on.
	Integrate with the national crisis management and CIIP plans.
	Where feasible, aim at the legal status of a CIIP coordinator.
	Use international expert forums and projects for collecting know-how and getting assistance.
	Task: Identify the goals
	Decide whether your scheme will address cybersecurity incidents, network faults, or both.
	○ In the cybersecurity area, use CERTs and CERT-like structures to receive incident reports and coordinate incident response across network operators, users and other stakeholders.
	○ In the network faults area, pay attention to defining the scheme's purpose correctly to suit your objectives.
	Decide what purpose or purposes of your scheme: emergency response, failure prevention, or legal rectification?
	○ For emergency response, target at cooperation of major CI providers, use an efficient communications tool, coordinate with public crisis management, coordinate across sectors.
	○ For failure prevention, consider both peer-to-peer cooperation and/or supervisory evaluation and recommendations as the main tools.
	○ For rectification, establish follow-up procedures after individual incidents, and make sure that a legal framework for this kind of regulation is provided.
	Task: Define basic requirements
	Select those who should report incidents.
	○ Involve large service providers into every kind of scheme.
	○ Smaller SPs may be excluded or charged with lesser reporting requirements.
	○ For cybersecurity CIIP, key end-users should also report.
	○ Remain open to spontaneous report from media and the public.
	Determine the reporting obligation of your scheme
	○ Rectification-focused reporting requires legal backing.
	○ If formulating a legal obligation, be brief; follow up with specific implementation.
	○ Obligation is not enough; keep cooperating with the reporting parties.
	Set reporting threshold(s); have a clear idea of the kind of incident that should be reported.
	○ For emergency response and cybersecurity, consider need of assistance as a threshold criterion.

Status	Task/Recommendation
	○ For emergency response, consider impact on CI providers as a threshold criterion.
	○ For failure prevention and rectification, consider impact on customers as a threshold criterion; you may combine number of customers affected, area, and duration of the outage.
	○ For rectification, consider social and political impact of an incident as a threshold criterion.
	○ Adjust reporting thresholds to the scheme's purpose: e.g. higher thresholds for emergency response and lower thresholds for statistics, failure prevention.
	○ Avoid low thresholds unless you are able to process a large volume of reports; also consider burden to the reporting parties to participate.
	○ Focus on flexible situation assessment in emergency response schemes.
	○ Aim at formalized thresholds in failure-prevention schemes.
	○ Cultivate shared understanding of what should be reported and why with the reporting parties.
Stage: Engaging Cooperation	
	Task: Start with what already exist
	Map the already existing arrangements for incident reporting, emergency response, industry cooperation, and CIIP, and build on them, if possible.
	Leverage the local culture of cooperation.
	Task: Formulate the value proposition
	Clearly formulate the expectations, possibilities, and value proposition of the scheme.
	Formulate advantages to the participants; consider in particular:
	○ efficient and fast information distribution;
	○ access to information unavailable elsewhere;
	○ information broking;
	○ assistance in emergencies;
	○ improved reaction to crisis situations.
	Task: Raise awareness
	Be pro-active in raising awareness about the needs for the scheme.
	Demonstrate your scheme's advantages to the participants.
	Secure C-level management support.
	Educate the potential reporting staff.
	Task: Build trust with the reporting parties
	Show serious commitment to the project.
	Build on previously existing trusted relationships.
	Use an individual, differentiated approach to the partner organizations.
	Invite the reporting parties and other stakeholders to get involved in the scheme's development.
	Task: Address the private stakeholders' concerns
	Establish clear rules on how will the submitted information be treated.
	If necessary, separate emergency reporting from the regulatory loop.
	Maintain confidentiality on network topology and other information that might be used in business competition.
	Anonymize public communication on incidents.

Status	Task/Recommendation
	Offer incident reporting as a channel to improve communication with customers.
	Promote information sharing as a way to increase efficiency and reduce cost of the participants' business continuity processes.
	In the network fault area, contribute to the costs of upgrades, if required.
	Balance your reporting requirements with the load they place on reporting parties' resources.
	Do not require too much reporting while the stakeholders are responding to the incident.
Status	**Task/Recommendation**
Stage: Setting The Reporting Procedure	
	Task: Set the reporting requirements
	Prepare a list of reportable information, including:
	○ contact information;
	○ time and location of the incident;
	○ status information;
	○ incident description;
	○ incident impact; and
	○ incident handling description.
	Use categorized variables in order to assist incident prioritization.
	Use unique incident ID for managing larger volumes of updating reports.
	Standardize the reporting format if a large number of reports is expected or if statistical analyses are planned.
	Automate for very large volumes of reports.
	Widely publicize the selected reporting channels among your constituency.
	Introduce your scheme as the single point of contact for reporting incidents within the eCommunications sector.
	Retain informal procedures for low reporting volumes and for emergencies.
	Invite quick alerts through any channel; keep alternative channels for emergency reporting.
	Have the initial report filed as soon as possible; updates can be sent later.
	Ask for the most detailed information in a concluding report.
	Consider a secure and resilient voice bridge as a tool for emergency response.
	Offer assistance to the reporting parties: issue guidelines, keep clarifying the requirements in informal communication.
	Task: Introduce prioritization mechanisms
	Use human review to prioritize incidents in any scheme that requires follow-up action.
	Use thresholds and in-built categorization as pre-filters in schemes with large volumes of reports. Even in that case, use human review.
	If using in-built categorization, consider differentiated deadlines for reporting, with the most severe incidents reported in the shortest time.
	For emergency response, maintain a 24/7 service to review incident reports.
	Task: Establish follow-up procedures
	Set procedures for information updating.
	○ In emergency response schemes, update the incident information and status continuously until the incident is closed.
	○ Use informal follow-up calls to complete the information with the reporting

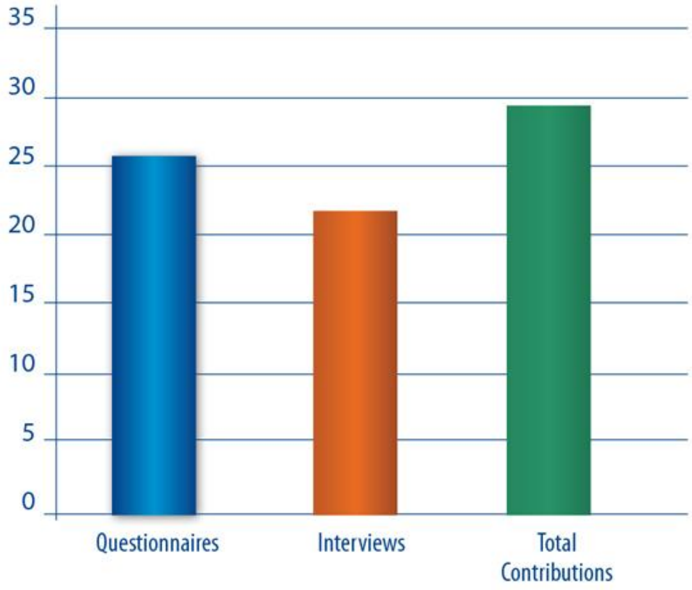
Status	Task/Recommendation
	parties.
	○ Provide additional information of the incident from CIP and emergency response sources.
	○ Invite real-time information sharing among the afflicted parties.
	Ensure that your scheme and its managers can reliably and effectively cooperate in emergency response.
	○ Monitor obligations stemming from legal norms or national crisis management plans.
	○ Prepare emergency communication guidelines, including an up-to-date contact list.
	○ In involving other bodies, follow the principles of subsidiarity and distribution economy.
	○ Exercise cooperation and communication in emergency situations.
	○ In case of an emergency, identify the incident responders by assessing the scope and impact of an incident.
	○ For complex incidents, assist the emergency responders by identifying the incident owner(s).
	○ If required, moderate communication between emergency responders and the eCommunications sector.
	Ensure effective information distribution within the scheme.
	○ Assign resources to manage information distribution following an incident
	○ Host communication bridges for intensive cooperation.
	○ Maintain up-to-date contact lists for delivering alerts
	○ Consider using automatic information distribution tools.
	○ Launch public alert sites for large constituencies.
	Channel assistance to the participants responding to an incident.
	○ In network faults area, focus on mediating mutual support between stakeholders and assistance from third parties.
	○ In the cybersecurity area, develop capacities to offer assistance in incident handling: analysis, consultations, on-site help, etc.
	Task: Ensure a suitable media policy and capabilities.
	Monitor media coverage, especially for rectification and regulatory purposes.
	Elaborate media policy and train/employ staff for answering media queries.
	Use media actively for distributing information about serious incidents or countering rumours and panic.
	Develop a long-term media strategy for continuous awareness raising.
Stage: Managing The Reporting Scheme	
	Task: Individual incidents' analysis and follow up
	Collect post-incident reports.
	Analyze novel incidents; react to the challenges by updating the scheme.
	Use incidents as an opportunity to educate the reporting parties:
	○ Follow-up with the incident owners.
	○ Issue alerts and exemplary lessons for the constituency.
	Ensure rectification where entitled to.
	Use synergy with the service providers' spontaneous tendency to secure business

Status	Task/Recommendation
	continuity.
	Task: Perform statistical analysis of reporting data
	In the cybersecurity area, organize automatic summaries on attacks.
	In the network faults area, aim at periodical in depth analyzes.
	Support the analysis with enough resources, both human and technical.
	Combine incident reports with data gathered from other sources.
	Enrich the reporting format so that more correlations may be performed.
	Task: Manage your scheme on a long term
	Consider the scheme as an evolving organism.
	Regularly collect feedback from the stakeholders.
	Educate the constituency and maintain their commitment.
	Improve the ex-post analyses and the value given back to the constituency.
	Consider expanding the scheme's coverage:
	o Extend the operation time to 24/7.
	o Enlarge the constituency.
	o Lower the reporting thresholds.
	o Enrich the reporting template.
	Formalize the reporting requirements, where applicable.
	Put aside time for tuning the scheme after introducing new requirements.
	If the purpose of reporting expands, consider expanding your role in the CIIP and/or incident response:
	o Promote to a national / governmental CERT.
	o Include CERT functions into the operations of a CIP authority;
	o Strengthen CIP or regulatory powers of a national CERT;
	o Federate functions within a telco regulatory authority.
	Still, consider running reporting schemes separately if it benefits their functions.
	Support integration to the national CIIP policy with legal framework adjustments.

9 Appendix B: Profile of Participants

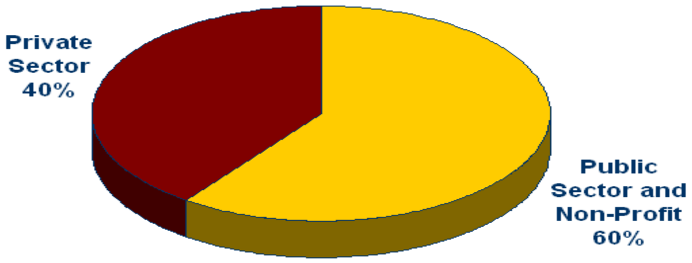
We have collected twenty-seven questionnaires and conducted twenty-five interviews. From some respondents we only had either the questionnaire or the interview. Altogether our research has covered thirty-one organizations or organization bundles (cases). It has been one of the priorities of the research to ensure that a wide spectrum of perspectives be represented. We have sought to include opinions from both private and public sectors, and from a variety of national and international contexts.

Figure 7: Organizations Participating in the Research, by Type of Contribution



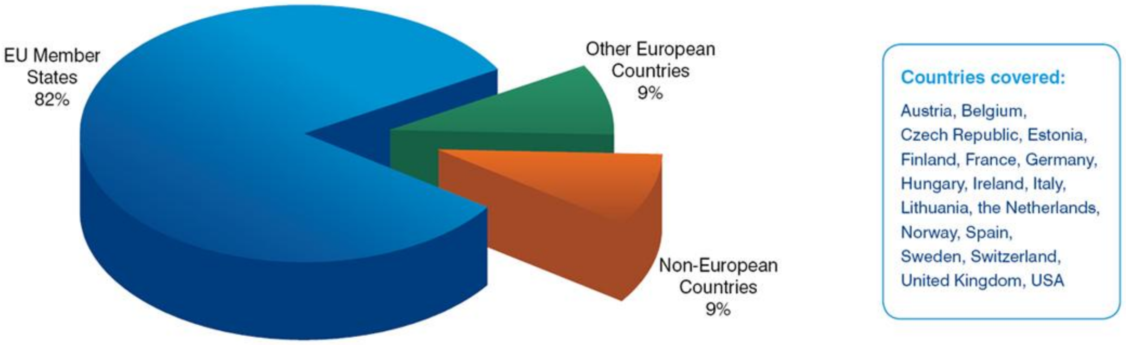
We have gathered input from twenty-one public organizations on seventeen cases (some organizations provided shared input on a single case). Our partners ranged from research networks via publicly owned postal services, national CERTs and CIIP authorities, telco regulatory authorities, ministries and government departments, up to organizations operating at the European Community level. We have also received opinions of nine service providers or business associations in eCommunications: typically, our respondents here were representatives of the former national incumbent companies. Finally we have been in touch with five software and/or ICT equipment vendors.

Figure 8: Organizations Participating in The Research, by Public and Private Sector



Geographically, most of our respondents were located within the EU, where we have covered organizations with headquarters in Austria, Belgium, Czech Republic, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, Spain, Sweden, the Netherlands, and the United Kingdom. In addition to that we also spoke to organizations with headquarters in Norway and Switzerland, plus the USA. Most of our respondent referred to a specific national reporting environment, though some were able to make international comparisons, too.

Figure 9: Headquarters of Organizations Participating in the Research



10 Appendix C: Resources

General Documents

COM(2009) 149 "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience," Communication from the Commission to the European parliament, the Council, the European Economic and Social committee and the Committee of the Regions, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT]

COM(2006) 251 "A strategy for a Secure information Society – "Dialogue, partnership and empowerment"", Communication from the Commission to the European parliament, the Council, the European Economic and Social committee and the Committee of the Regions, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT]

ENISA NSIE Guide. "Good Practice Guide: Network Information Security Information Exchanges." [http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide]

CERT Guidelines

ENISA. "CSIRT Setting up Guide". ENISA has formulated a guide for setting up CSIRTs for single organizations, whole sectors, or on the national level. [http://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide]

GOVCERT.NL "CERT-in-a-box," "Alerting-service-in-a-box". Summary of the lessons learned during setting up GOVCERT.NL and the Dutch national Alerting service. [http://www.first.org/resources/guides/cert-in-a-box/]

NIST Incident Handling Guide. Tim Grance, Karen Kent, Brian Kim: "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology," (January 2004). The Guide provides guidance on cybersecurity incident handling, incident reporting inclusive. [http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf; http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf]

CERT.FI "National and Governmental CSIRTs in Europe" In October 2009 CERT.FI conducted an overview of eleven CSIRTS and GovCERTs in Europe, including some ideas on their typical functions and evolution strategies. [http://www.cert.fi/attachments/certtiedostot/5kiBC9Qy0/National_and_Governmental_CSIRTs_in_Europe.pdf]

CERT/CC "Steps for Creating National CSIRTs". CERT/CC suggests steps to organize a national CERT/CSIRT. [http://www.cert.org/archive/pdf/NationalCSIRTs.pdf]

Regulatory Decrees

FICORA "Regulation On Obligation to Report Information Security Incidents and Faults and Disturbances in Public Telecommunications" (Under Revision). [http://www.ficora.fi/attachments/englantiav/5hw9MAxqr/FICORA09C2009M.pdf]

OFTA. "Guidelines for Cable-Based External Fixed Telecommunications Network Services Operators and Internet Service Providers for Reporting Network and Service Outages" [http://www.ofta.gov.hk/en/report-paper-guide/guidance-notes/gn_200802.pdf]

FCC. Code of Federal Regulations, Title 47, Volume 1, Part 4, Sec. 4 [http://frwebgate4.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=646530369015+11+2+0&WAISaction=retrieve]

Reporting Forms

FICORA Form for Reporting Faults and Disturbances in Communications Networks and Services
[http://www.ficora.fi/attachments/englantilomakkeet/1156489300308/VIe.pdf]
CERT-FI CERT-FI Incident Report
[http://www.ficora.fi/attachments/englantilomakkeet/1156489299995/TIe.pdf]
ICS Incident Briefing Form (ICS 201)
[http://training.fema.gov/EMIWeb/IS/ICSResource/assets/ics201.pdf]
ICS Incident Status Summary (ICS 209)
[http://training.fema.gov/EMIWeb/IS/ICSResource/assets/ics209.pdf]
NORS Network Outage Reporting System User Manual, Version 6 (April 2009),
[http://www.fcc.gov/pshs/outage/nors_manual.pdf]

Other Materials

MIMER/GLU. The Swedish national reporting system is currently progressing towards its Transnational Dissemination stage. For basic information and contact, see [http://www.pts.se/upload/Faktablad/En/facts-about-glu.pdf].
NORS and DIRS. FCC offers brief description of its reporting systems with further links.
[http://www.fcc.gov/pshs/services/cip/nors/nors.html;
http://www.fcc.gov/pshs/services/cip/dirs/dirs.html]

11 Appendix D: Questionnaire

STRATEGY

Do you have a national incident reporting scheme? Please describe the strategy behind the scheme, and how it was developed.

Is this part of a more general national crisis management strategy? Please describe.

Is incident reporting mandatory or voluntary in your country? What incentives are given to operators and service providers to report incidents?

REPORTING

How do you define and prioritise incidents?

What are the reporting requirements for each category of incidents (including format of report, timing requirements, stages of reporting)?

Which authorities/organizations are involved when an incident occurs? What are their responsibilities and duties?

How do you handle cross-sector incidents (such as those involving power supply and telecommunications)? How do you resolve co-ordination issues?

What is the role of media during an incident reporting life - cycle?

POST INCIDENT HANDLING

Is there an ex post assessment (of incident notifications) procedure in place? Please describe.

How do you ensure that operators/service providers learn from the experiences of serious incidents and update their measures accordingly?

Are there any liabilities or punishments for parties involved in an incident due to improper provision of measures? Under which conditions?

PROBLEMS AND SUGGESTIONS

What are the major problems/barriers (if any) in running a security incident scheme? - how did you solve them?

Are there any things which you would change or improve in the incident reporting scheme?

What main piece of advice would you give to someone just starting out to design an incident reporting scheme?

Please tell us if you feel we have missed out any important questions or subject areas which should be addressed when producing the good practice guide.

12 Appendix E: Definitions

Business Continuity

Availability of critical business functions to customers, suppliers, regulators, and other entities that must have access to those functions. Business continuity is ensured by a range of means and activities that foster availability and recoverability of services, such as: business continuity planning; guaranteed services and/or supplies from suppliers and subcontractors; internal backup and recovery policies; procedures for change control and project management; and customer support. [IDC]

Business Continuity Planning

Creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Computer Emergency Response Team (CERT)

A Computer Emergency Response Team (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The team provides the necessary services to handle them and support their constituents to recover from computer security breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency. The constituency (an established term for the customer base) of a CERT usually belongs to a specific sector, like academia, companies, governments or military. The term CSIRT (Computer Security Emergency Response Team) is a more modern synonym and should reflect the fact that CERTs developed over time from being mere reaction forces towards more universal providers of security services. [ENISA]

Computer Security Emergency Response Team (CSIRT)

See Computer Emergency Response Team

Crisis Management

See Emergency Management

Crisis Response

See Emergency Response

Critical Infrastructure (CI)

Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. [COM(2004) 702]

Critical Information Infrastructure (CII)

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.). [COM(2005) 576]

Cybersecurity

Computer technology and related processes focused on protection of information and services on electronic communications networks or information technology from theft, tampering or disruption by unauthorized activities or untrustworthy individuals and unplanned events respectively. [IDC]

Distributed Denial of Service (DDoS)

An explicit attempt to render a computer or a network incapable of providing normal services, performed via coordinated attack from multiple locations. DDoS attackers compromise a number of end-hosts (typically using a virus or worm) or routers, and then use those compromised hosts to flood the bandwidth or resources of a targeted system, thus making it unavailable to the intended users. [W3C, Internet Architecture Board, CERT/CC]

Electronic Communications (e-Communication) Network

Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. [Directive 2002/21/EC].

Emergency

An event or situation which threatens serious damage to human welfare or to the environment; also an act of war or terrorism which threatens serious damage to the national security. [Emergency Response and Recovery: Non Statutory Guidance Accompanying The Civil Contingencies Act 2004; ver 2, August 2009]

Emergency Services

Organizations which ensure public safety by addressing different emergencies. [IDC]

Emergency Management, also Crisis Management

Emergency management is the continuous process by which all individuals, groups, and communities manage hazards in an effort to avoid or ameliorate the impact of disasters. For the purposes of this guide, emergency management refers to publicly coordinated emergency management and to the authorities which are in charge of it. [IDC]

Emergency Response, also Crisis Response

The process of immediate reaction to a large scale emergency. For the purposes of this guide, emergency response refers to publicly coordinated emergency response. [IDC]

Governmental CERT (GovCERT)

A CERT that is responsible for the protection of governmental and/or administrative networks. The constituency of a governmental CERT therefore is the government and other public bodies. Exact definitions of GovCERT roles may vary across the EU Member States. In many cases a governmental CERT also acts as national CERT (see definition). [ENISA]

Incident

An event which may harm or threaten, either directly or indirectly, the resilience and security of public eCommunication networks. NB that data protection incidents (security breaches etc.) are explicitly considered outside of the scope of this study. [ENISA and IDC]

National CERT

A CERT that acts as national point of contact for information sharing (incident reports, vulnerability information and other) with other national CERTs in the EU Member States. National CERTs can also be considered as "CERTs of last resort", which is just another aspect of their role as a unique national point of contact with a coordinating role. In a lot of cases a national CERT also acts as governmental CERT (see definition). [ENISA]

Public Communications Network

An electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. [Directive 2002/21/EC]

Public-private partnership (PPP)

A cooperative venture between the public and private sectors, built on the expertise of each partner, that best meets clearly defined public needs through the appropriate allocation of resources, risks and rewards. For the purposes of this Guide, private-public partnerships include also activities beyond mere economic contracts, such as CIP projects. [Canadian Council of Public-Private Partnerships, IDC]

Resilience

The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation.

13 Appendix F: Abbreviations

BKA	Bundeskanzleramt Österreich [Austrian Federal Chancellery, AUT]
BSI	Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security, DE]
CERT	Computer Emergency Response Team (see the definition above)
CI	Critical Infrastructure (see the definition above)
CII	Critical Information Infrastructure (see the definition above)
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
ComReg	Commission for Communications Regulation [IRL]
CONOPS	Concept of Operations [UK]
CSIRT	Computer Security Incident Response Team (see the Computer Emergency Response Team definition above)
DDoS	Distributed Denial of Service (see the definition above)
DIRS	Disaster Information Reporting System [USA]
DSLAM	Digital Subscriber Line Access Multiplexer
EPCIP	European Program for Critical Infrastructure Protection
FICORA	Finnish Communications Regulatory Authority [FI]
GLU	Gemensam lägesuppfattning [Joint Situation Assessment, SE; same as MIMER]
GovCERT	Governmental CERT, Government Computer Security Response Team (see definition above)
GPS	Global Positioning System
ICS	Incident Command System
ICT	Information and Communication Technologies
ID	Identification
INTECO	Instituto Nacional de Tecnologías de la Comunicación [National Institute of Information Technologies, ESP]
ISE	Information Sharing Environment
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technologies

ITIL	Information Technology Infrastructure Library [UK]
IT-ISAC	Information Technology Information Sharing and Analysis Center [USA]
MELANI	Melde und Analysestelle Informationssicherung [Reporting and Analysis Centre for Information Assurance, SUI]
MIMER	Multipurpose Information Management and Exchange for Robustness [SWE; same as GLU]
MinEcon	Ministry of Economic Affairs [NED]
NCS	National Communications System [USA]
NEAT	National Emergency Alert for Telecoms [UK]
NEISAS	National and European Information Sharing and Alerting System
NHH	Nemzeti Hírkölési Hatóság [National Communications Authority, HU]
NIST	National Institute of Standards and Technology [USA]
NORS	Network Outage Reporting System [USA]
NPT	Norwegian Post and Telecommunications Authority [NO]
NSIE	Network Information Security Exchange
NTCG	National Telecommunications Crisis Management Coordination Group [SWE]
OFTA	Office of The Telecommunications Authority [Hong Kong]
PTS	Post och telestyrelsen [Swedish Post and Telecom Agency, SWE]
PPP	Public-Private Partnership (see the definition above)
RRT	Ryšių reguliavimo tarnyba [Communications Regulatory Authority of the Republic of Lithuania, LT]
SMS	Short Message Service
SP	Service Provider
SPOC	Single Point of Contact
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen [Implementation Plan of Critical Infrastructures, DE]
WARP	Warning, Advice and Reporting Point
XML	Extensible Markup Language