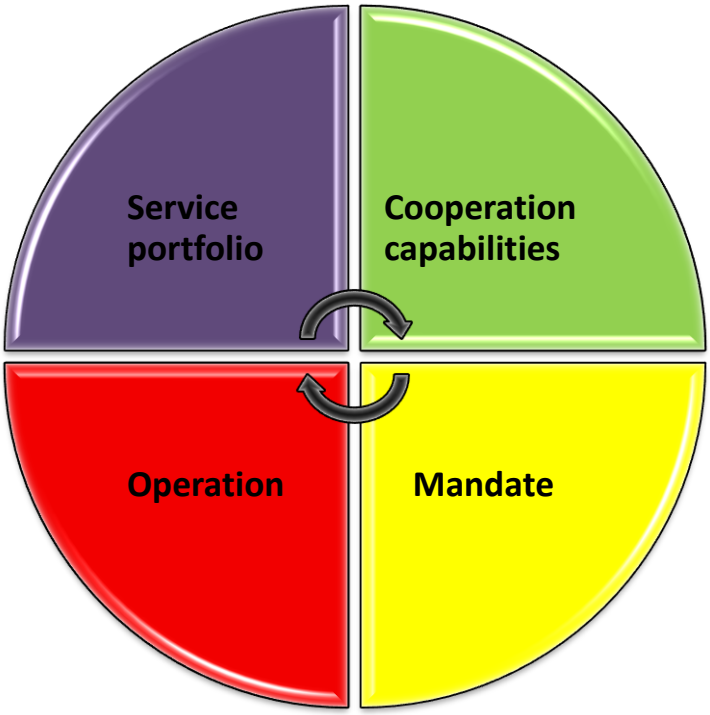
Baseline capabilities for national / governmental CERTs



Version 1.0 (initial draft)

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For contacting ENISA or for general enquiries on CERTs, please use the following details:

e-mail: Marco Thorbruegge, cert-relations@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Table of Contents

Executive summary

This document constitutes a very first attempt to define a minimum set of capabilities that a Computer Emergency Response Team (CERT) in charge of protecting critical information infrastructure (CIIP) in the Member States should possess to take part and contribute to a sustainable cross-border information sharing and cooperation. In areas where no clear statements can be made with regards to requirements the document points out recommendations and areas for further analysis in the future.

This first version was derived from the answers to a survey ENISA carried out among all 120+ publicly listed[1] CERTs in Europe. It should be considered only as a first step towards the specification of requirements, which is an ongoing process that has and will involve discussions with the relevant stakeholders in the Member States.

Introduction

This document covers recommendations and proposals for capabilities of so called national / governmental CERTs, thus teams who serve the government of a country to protect critical information infrastructure. National / governmental CERTs play a key role in coordinating incident management with the relevant stakeholders at national level. In addition they bear responsibility for cooperation with the national / governmental teams in other countries.

At the moment of writing only roughly 50% of the EU Member States have an established, functional national / governmental CERT at their disposal, with ongoing projects to set-up such a team in almost all other Member States. In addition to that deficiency the capabilities (in areas like operational equipment, service portfolio, cooperation capabilities, official framework / mandate by the government and others) vary substantially among the already established teams.

It is beyond doubt that protection of critical information infrastructure (CIIP), like the internet itself, does not stop at national borders. It is also beyond doubt that in order to effectively and efficient respond to threats and attacks against information infrastructure a coordinated approach at European level is needed. One way to facilitate that goal is to support the Member States in enhancing cooperation among national / governmental CERTs, with regards to information sharing and coordinated incident response.

Due to the diversity in capabilities mentioned earlier, a Europe-wide cooperation among national / governmental CERTs, involving stakeholders in all Member States, does not yet exist. However, there are activities and initiatives for information sharing and incident response, which work quite well in practice, and some of them are already active for

[1] *ENISA inventory of CERT activities in Europe:* http://www.enisa.europa.eu/act/cert/background/inv

years. One example is the Financial ISAC initiative (FI-ISAC), where experts from national / governmental CERTs, law enforcement and the banking sector regularly share information about threats and vulnerabilities in order to better protect the financial sector. Another example is the European Government CERT group (EGC)[2], an informal group of mature national / governmental CERTs that have been sharing operational information on a day-to-day basis already since 2001. The experiences gained from these activities provide very valuable insight into cross-border cooperation and the requirements and the obstacles for sustainable information sharing. All future actions at European level to foster cooperation among national / governmental CERTs must take into account experiences made within these successful activities.

The key problem of cross-border cooperation we face at the moment is the diversity of capabilities, resulting from either the (1) complete lack of a national / governmental CERT in some Member States or (2) the lack of what is perceived as an "adequate level of maturity", supported by baseline capabilities of the teams that exist in some other Member States.

ENISA is addressing the first (1) issue by constantly advocating the need for the establishment of national / governmental CERTs in the Member States, and supporting these projects with expertise, training and exercises for CERTs.

This document is the first approach towards a definition of baseline capabilities for national / governmental CERTs in order to address the second (2) issue in almost 21 years of worldwide CERT history.

In 2009 ENISA carried out a comprehensive survey among all publicly listed[3] CERTs in Europe, in order to get a better idea of what the CERT community considers as an "adequate level of maturity" or "baseline capabilities", especially for national / governmental CERTs. An emphasis was put on the question "What do you consider as requirements and obstacles to information sharing with teams in other countries". This document reflects the answers to the survey.

---

[2] *European Government CERT Group:* http://www.enisa.europa.eu/act/cert/background/inv/cert-activities/co-operation

[3] *ENISA inventory of CERT activities in Europe:* http://www.enisa.europa.eu/act/cert/background/inv

Disclaimer

The document in its current status is by no way to be considered final. In some areas of capabilities of national / governmental CERTs the proposed requirements are quite stable, while in other areas additional research, analysis and comprehensive discussions with the involved stakeholders are necessary. This document is to be considered "work in progress"!

Having a national / governmental CERT in place that fulfils the requirements for "baseline capabilities" defined in this document is essential for CIIP in all Member States. However these teams should not be considered as the one and only necessary measure a Member State must take in order to assure adequate protection. CIIP at national level must always be planned within a complete cyber security strategy, in which a national / governmental CERT is an important part, but not the only one. The planning of a complete national cyber security strategy in a Member State is outside the scope of this document; however it provides an insight into what role these teams can play and how they could be embedded into such strategy.

Glossary

CERT / CSIRT

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 Incident 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.

National CERT

Informal definition: a CERT that acts as national point of contact (PoC) for information sharing (like incident reports, vulnerability information and other) with other national CERTs in the EU Member States and worldwide. National CERTs can be considered as "CERT of last resort", which is just another definition of a unique national PoC with a coordinating role. In a lot of cases a national CERT also acts as governmental CERT. Definitions may vary across the EU Member States!

De facto national CERT

Informal definition: de facto national CERTs act as PoC in countries where no official national CERT has been established yet by the government. Usually the first CERT established in a country is perceived as de facto national CERT by teams in other countries. "De facto national CERTs" are indispensible for cross-border incident management, until an official national CERT is established, or the former "de facto national CERT" is officially mandated by the government. De facto national CERTs are not in the scope of this document.

Governmental CERT

Informal definition: a CERT that is responsible for the protection of governmental / administrative networks. The constituency of a governmental CERT therefore is the government and other public bodies. In a lot of cases a governmental CERT also acts as national CERT. Definitions may vary across the EU Member States!

The term national / governmental CERT

The informal definitions for "national CERT" and for "governmental CERT" do not uniquely reflect the status, role and responsibility of all the CERT teams ENISA tries to address. In the context of this document and ENISAs work in the area of baseline capabilities the term "national / governmental CERT" is introduced. Still vague, this term depicts the following kind of CERT:

- acting as official[4] national point of contact for national / governmental CERTs in other Member States
- bearing responsibilities for the protection of critical information infrastructure (CIIP) in its country

The term "national / governmental CERT" therefore subsumes all "flavours" of national CERTs, governmental CERTs, national points of contacts and others in the EU Member States.

Acronyms

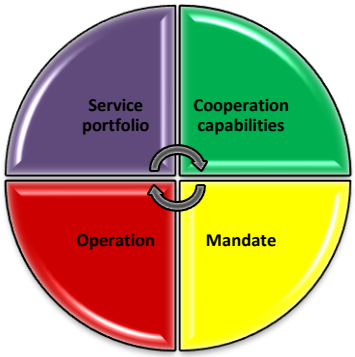
CIIP	Critical Information Infrastructure Protection
EGC	European Government CERT (Group)
FI-ISAC	Financial Information Sharing and Analysis Center
FTE	Full Time Equivalent
IXP	Internet Exchange Point
NIS	Network & information Security
PGP	Pretty Good Privacy
PoC	Point of Contact
SMS	Short Message Service

[4] *Mandated by the government of the respective EU Member State*

Baseline capabilities for national / governmental CERTs

The following text will outline harmonized proposals for a baseline set of capabilities for national / governmental CERTs in the Member States in four categories:

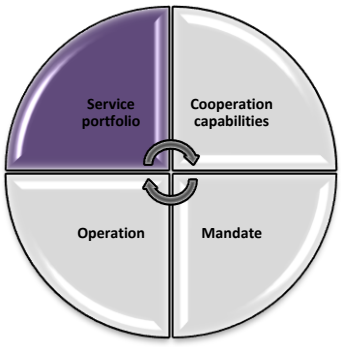
- **Service portfolio** covers the services that a team provides to its constituency or is using for its own internal functioning
- **Mandate / official framework** covers the powers and justification that need to be granted to the team by the respective government
- **Operational capabilities** covers technical and operational requirements a team must comply with
- **Cooperation capabilities** subsumes the requirements with regards to information sharing with other teams, that are not covered by the previous three categories



Service portfolio

External services

Out of the list of CERT services[5] **Incident Handling, Analysis and Reporting** (subsumed under **Incident Management**) is the only service that must be considered a mandatory core activity and a service that each national / governmental CERT must provide for its constituency. On top of this it is advisable to provide **Alerts and Warnings** and **Announcements** for the constituency in a both reactive and proactive way. **Sharing of security related information** on alerts and warnings in immediate cases of upcoming threats or other emergencies, and good user practice for mid- and long-term awareness building provide measurable added value for the constituency, with low effort and cost involved. Security notifications and other information for the constituents also greatly



[5] *CERT services list from CERT/CC:*
http://www.enisa.europa.eu/act/cert/support/guide/appendix/csirt-services

improve the visibility and the standing of a CERT, and facilitate the building of trust in the capabilities of a team.

Outsourcing

While Incident Management and Alerting are services that the national / governmental CERT must provide itself it is thinkable to outsource some of the less immediate, mid- and long-term services. More concrete recommendations will require further investigation and analysis.

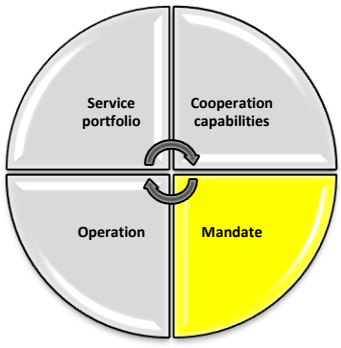
Internal functioning

For the internal functioning of a national / governmental CERT a couple of other services and measures should be implemented. In general it is necessary that a team at all times is aware of what is going on in the networks of their constituents, in their own networks, the networks of its partners and the "internet as a whole". Constant **situation awareness** is greatly improved by **technology watch, training** and **exercises**[6].

All other services from the list can in principle be considered optional and the provision is dependent on the need of the constituency.

Mandate / official framework

An **official mandate** by the government to represent the country in the CERT communities (like FIRST[7] and EGC) is crucial for a national / governmental CERT. This mandate must include provisions for the team to act as **official national Point of Contact (PoC)** for CERTs (and other members of the security community) in other countries as an indispensable element of the national CIIP plan and for a clear and flexible international collaboration.



In general it is advisable that a national / governmental CERT is established (and accepted) as a "**CERT of last resort**" that, in case of doubt and emergency, is available to relay incident reports (and other security related information) to the right stakeholders in its country.

---

[6] *See for example ENISA CSIRT exercise material:* http://www.enisa.europa.eu/act/cert/support/exercise

[7] *Forum of Incident Response and Security Teams:* http://www.enisa.europa.eu/act/cert/background/inv/initiatives-outside-europe/first

However, it is not necessary (and sometimes even counterproductive) that a national / governmental CERT is made responsible for the management of incidents for all stakeholders in a country. Instead it is recommended to investigate on national level an appropriate integration of the team to the national CIIP structure and existing CERT "landscape".

Good common practice of EU Member States for CERT mandating will be identified and published in 2010.

Role on national level

Definitely the "**status quo**" with regards to the relevant NIS key players in a country and their relationship **must be taken into account** when the mandate for the national / governmental CERT is formulated. A cooperative approach that includes all relevant stakeholders proved to be most successful in the past and greatly facilitates the acceptance of the national / governmental CERT, and helps it to grow into its role and responsibilities (see the paragraph "Operational capabilities").

Communication

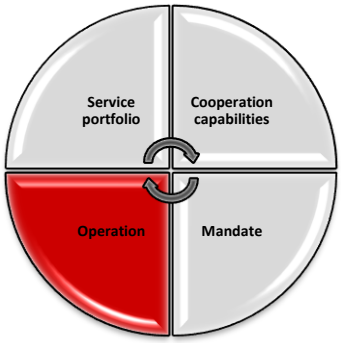
It is important that the **role and responsibility** of a national / governmental CERT is **clearly communicated** to all relevant stakeholders in other countries. All ambiguities and national / local peculiarities should be "hidden" from external stakeholders as much as possible, in order to avoid confusion and consecutive delays in the flow of information. It is important to encourage the Member States respectively their governments to make steps towards **simplifying** and **unifying** the legal framework for the national / governmental CERT. This includes specifying the team's duties, rights, responsibilities and mandate in order to create a common legal understanding within European Union.

Organisational model

For the organisational model it is recommended to evaluate the role of national / governmental CERTs in governmental structure to decide which sector, ministry, agency or other structure is the most appropriate place for the CERT in the particular country. More concrete recommendations will require further investigation and analysis.

Operational capabilities

Ressources



It is difficult to provide sensible requirements for the **(initial) size** of a national / governmental CERT, as various factors influence the number of staff. Taking experiences from the past a suitable size to start with seems to be **3 to 5 Full Time Equivalents (FTE)**, when services are provided during office hours only. In order to provide sustainable service levels at least a team leader, a Senior incident Handler for the triage and an additional technical expert is necessary. However for national / governmental CERTs with responsibilities for CIIP and (inter)national cooperation additional personnel should be foreseen from the beginning in order to provide adequate reachability (estimated 6 – 8 FTE)

Business hours

It is considered mandatory for a national / governmental CERT to provide a **reachability 24/7/365** for its own constituency and national and international cooperation partners. It depends on the service portfolio, structure and the responsibilities of the team to provide reachability either physically or by "call duty", but it is crucial to guarantee quick response times, especially for incident reports.

Communication services

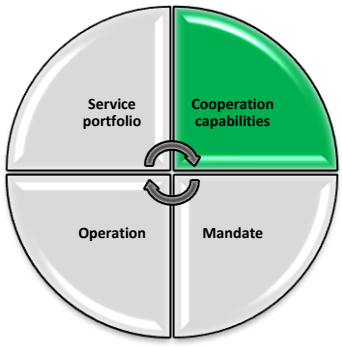
Telephone, **email** and a website are considered a minimum set of equipment. **Encrypted** emails for secure communication with the national / governmental CERT is necessary. PGP is still considered mandatory for every team, complemented by S/MIME where appropriate. The possibility to access the team's website via encrypted connection is mandatory as well when confidential data can be submitted (i.e. when the team provides web-forms to report incidents).

Physical security

An often underestimated factor is **physical security**: as a national / governmental CERT naturally deals with sensitive information that needs to be protected, adequate measures must be taken to physically secure the workplace of a team. This is even more important as the CERT not only processes information from its own country but also sensitive information from other countries that is shared with the team. In addition adequate physical security provides means for trust building with cooperation partners during site visits.

Cooperation capabilities

A sustainable and effective cooperation on both national and international level is indispensable for the success of national / governmental CERTs. This is true not only during cases of emergency, but rather on a day-to-day operational basis.



In this regard three elements are considered crucial for national / governmental CERTs:

- Trust and trust building
- Quality and sustainability of information and reaction
- Common terminology and schemes

Trust and trust building

Trust and trust building is a very complex topic with various influential factors, so it is very difficult to define concrete requirements in this area. It's more promising to formulate (rather vague) **recommendations** for national / governmental CERTs, good practice that is derived from more than 20 years of experience of CERT cooperation. Further research is necessary in order to achieve a better understanding in this area.

Personal knowledge

Personal knowledge and reputation is still considered the number one criteria for trust building and, in consequence, for successful cooperation. This is why **integration** into the relevant **CERT communities** (FIRST, TF-CSIRT[8], etc.) is crucial. Teams need to gain good reputation through their behaviour, actions and involvement over the time, and this team reputation (which is by no means a measurable factor) is closely linked to the reputation the single team members have. Without this reputation it is very difficult for a team to establish fruitful cooperation with other teams, or even join existing cooperation activities. Reputation, however, can be "inherited" in two ways: a good reputation of a single team member results in good reputation for the whole team. And a team (or a single staff member) with a good reputation can introduce new teams into established cooperation activities (vouching). However then the new team still has to build up its own good reputation over time, but the first hurdle of introduction is taken.

[8] *Task Force of Computer Security and Incident Response Teams:* *http://www.enisa.europa.eu/act/cert/background/inv/cert-activities/co-operation*

Reputation

There is no "golden rule" for building up a good reputation. Integration into the existing CERT communities is necessary. A (pro) active role in discussion and projects initiated during meetings is an important supporting factor. Proven technical expertise and a general sensible appearance of team members greatly improve reputation. And last but not least a team and its members must prove to be reliable and discreet. Again: trust between teams is built over time (but can be destroyed in a few seconds of carelessness), and personal knowledge and mutual appreciation are the key factors.

Informal groups

Interestingly enough informal cooperation and information sharing activities are considered the most fruitful by the participants, and (at least at the moment) seem to be preferable to formal constructions. As a matter of fact when more than two parties are involved in an activity informal groups like the EGC have a couple of advantages and offer the participants more flexibility. While formal structures support Standard Operating Procedures and the liability of what is done, it definitely needs to be explored further if and how more formal structures can complement informal structures and improve cooperation and information sharing.

National vs. International cooperation

All of the above mentioned principles are also valid for a successful cooperation and information sharing on national level. Clearly a national / governmental CERT should play a key role in organising and coordinating cooperation with the relevant key players in its country. Only with a good functioning cooperation on national level a national / governmental CERT can fulfil its role on international level, where it is considered as the national PoC for information sharing. Building a community of key players for NIS and CIIP on national level should be a paramount goal for each national / governmental CERT.

Quality and quantity of information

Information sharing among national / governmental CERTs can only be successful over time if two requirements are met: all involved parties contribute, and the level of quality of provided information is (more or less) equal among all participants. The first requirement obliges CERTs that take part in information sharing activities to contribute information in order to "deserve" to receive something back. The second requirement suggests that the other parties must benefit from the information shared by a team. Both factors together suggest that a national / governmental CERT must meet the other partners on "eye-level", with the ability to provide added value by sharing important information that is either unknown to the others, or that helps to back up own observations. Again these are rather immeasurable requirements that must be adjusted over time, but experience shows that neglecting them will, sooner or later, lead to exclusion of cooperation partners or to the abandonment of a whole information sharing activity.

Sustainable reaction

Another important factor is the kind of reaction a national / governmental CERT is able to provide to information it receives, which is especially true for incident reports. In an ideal case a team is able to immediately act on an incident report from another team and, for example, cut an attacking system off the network. This is only possible if the national / governmental CERT has direct access to core infrastructure like IXPs (which is not often the case) or has a mandate to instruct the ISPs in its country to do so. But even such mandate is not often given to national / governmental CERTs and so again the importance of a well-functioning cooperation on national level needs to be emphasised. A well-established cooperation among all key players in a country like CERTs, ISPs and other stakeholders, built on trust and the will to cooperate can mitigate effectively the lack of access to core infrastructure, either directly or indirectly via mandate. A CERT that can only receive incident reports about its constituency, but is not able to timely and sustainably react to them, cannot fulfil its obligations as a national / governmental CERT, and will sooner or later be excluded from information sharing.

Common terminology and schemes

It is rather self explaining that information sharing only works if a common understanding of the topic and the used terminology among the partners is present. This helps to avoid ambiguities and, as a consequence, wrong reactions. National / governmental CERTs involved in cross-border cooperation and information sharing also have to follow similar procedural schemes, for example for the classification of information or for the encryption of information. It is always advisable to review good common practice and apply them wherever appropriate (like agreeing on using PGP for encryption or classifying information according to the traffic light protocol proposed by CPNI in the UK).

History

12/2009: Version 1.0 – initial draft, based on a survey among 120+ European CERTs

Next steps

1. Incorporate findings of other studies, surveys, etc. into the documents (CERT-FI study, ENISA resilience stock taking, etc.
2. Split the document into three separate parts:
   - **Policy recommendations** in the context of national / governmental CERTs (target audience: EU Member States)
   - **Good practice for CERTs** and management (target audience: national / governmental CERTs and their management)
   - **Good practice for information sharing activities** (target audience: information sharing groups)

Areas and topics that require further investigation

Policy recommendations for EU Member States

Good practice in mandating national / governmental CERTs

This area covers the definition of roles, powers and responsibilities of national / governmental CERTs by a government in an EU Member State, with regards to CIIP, cross-border cooperation and national point of contact. Good practice for CERT mandating from the MS should be collected, consolidated and communicated as policy recommendations.

Good practice in coordination and cooperation on national level

- How to identify the NIS key players in a country?
- What is the role of a national / governmental CERT?
- Etc.

Starting points can be found in ENISAs report on "CERT cooperation and its facilitation by relevant stakeholders"

Good practice in operational models

This area covers the organisational environment for national / governmental CERTs. "Which part of the government is responsible for running the CERT", "Should a CERT be embedded in a hosting organisation" and other questions should be raised and answered. The way individual EU Member States deal with this topic should be assessed and several scenarios should be presented as alternatives and, where appropriate, communicated as policy recommendations.

Good practice for CERTs and management

Good practice in providing Incident Management

This area covers general practice on how to organise incident management, the core service for every CERT. Questions like "How to classify incidents (triage)", "how to organise incident tracking", "what timelines to choose for response", and others should be raised and answered. Main goal should be to support newly built teams. Secondary goal should be to encourage established teams to learn from each other.

Good practice in providing Alerts & Warnings

This area covers general practice in providing alerting and warning services ("security advisories"). Questions like "where to find timely information", "what sources can be trusted", "how to classify a vulnerability" and others should be raised and answered. Main

goal should be to support newly built teams. Secondary goal should be to encourage established teams to learn from each other and to find synergies.

Good practice in outsourcing of CERT services

- What experiences do CERTs have with outsourcing?
- How to keep control of the results?
- Which services can and which should not?
- Etc.

Good practice in "internal functioning"

- How do mature CERTs keep themselves "up-to-date"?
- How is "early warning" realised?
- What are the procedures to deal with incoming information?
- How are results presented to management and government?
- Etc.

Starting points can be found in ENISAs "CSIRT setting-up guide", the feasibility study for an "Europa wide Information Sharing and Alerting System" and the work of the ad-hoc working group "CERT services".

Good practice in coordination and cooperation on national level

- How to identify the NIS key players in a country?
- What is the role of a national / governmental CERT?
- How to develop a community?
- Etc.

Starting points can be found in ENISAs report on "CERT cooperation and its facilitation by relevant stakeholders".

Good practice in resource planning

- How many staff members does a CERT need for initial operation?
- How should the CERT grow when new services are planned?
- How to deal with peak times?
- Etc.

Starting points can be found in ENISAs "CSIRT setting-up guide"

Good practice for general service provision

- Which services provide what added value, and for which cost?
- Which services need to be provided 24/7, and which do not?
- What tools and equipment to use?
- Etc.

Starting points can be found in ENISAs "CSIRT setting-up guide" and the "Clearinghouse for Incident Handling Tools".

Good practice for data protection

- How to securely communicate sensitive data?
- How to process sensitive data securely?
- How to store and delete sensitive data?
- Etc.

Good practice on physical security

- What office location to choose for a CERT?
- How to "harden the building"?
- How to manage access?
- Etc.

Starting points can be found in ENISAs "CSIRT setting-up guide"

Good practice for information sharing activities

Enhanced mechanisms for trust building

In this area, where probably the most research effort is necessary, alternatives to "personal knowledge" and reputation based trust building between CERTs should be identified and assessed.

Starting point for this could be a pre-study with the same name that ENISA carried out in 2007.

Other areas of interest may be:

- Common operational schemes to facilitate cross-border cooperation
- Good practice on reputation building
- Information sharing - quality and quantity