CSIRT Capabilities

How to assess maturity?

Guidelines for national and governmental CSIRTs

FINAL

VERSION 1.6

PUBLIC

DECEMBER 2015

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Baiba Kaskina, Edgars Taurins, Andrea Dufkova.

Contact

To contact the authors please use cert-relations@enisa.europa.eu
For media enquiries about this paper please use press@enisa.europa.eu.

Acknowledgements

The authors would like to thank the following experts who took the time to be interviewed and whose opinions and views have contributed to findings and suggestions of this study; from Trusted Introducer experts – Don Stikvoort, Klaus-Peter Kossakowski and from national and governmental CSIRTs experts – Martijn de Hamer (NCSC-NL), Aart Jochem (NCSC-NL), Serge Droz (SWITCH CERT), Robert Jonsson (CERT-SE), Erika Stockinger (CERT-SE), Bryk Harri (NCSC-FI).

ISBN 978-92-9204-164-9, DOI 10.2824/214073

Table of Contents

Executive Summary

National and governmental CSIRTs are essential for every country that is concerned about protecting its digital assets, starting from sensitive government information to its citizens and their information. The CSIRTs' role is very wide, from security incident response and management to various sophisticated technical services and awareness-raising and educational activities. When dealing with cyber incidents, CSIRTs have to work closely with law enforcement and other authorities, but no other authority in the cyber ecosystem is in the better position to help users and institutions to stop cyber incidents, to understand why they could happen and what to do to prevent them from happening again; this is the unique role of a CSIRT.

Currently in the EU, governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure as well as to ensure cyber-crisis management. National CSIRTs, on the other hand, are playing different roles in different countries. In some countries they are responsible for the whole IP address space of that country, in others they also take the role of 'last resort' when no security contact point for an IP address can be found. In any case, when another country has to be contacted regarding solving an incident, national CSIRTs are often asked to help to find the right contact person. Increasingly CSIRTs expect other teams with comparable competences to react to their requests in a timely manner and to handle shared information professionally. A maturity process and certification can help to ensure that these expectations are met. A high level of maturity (certification or similar activities) is also desirable for successful participation in CSIRT cooperation networks working in Europe. Many governmental and national CSIRTs are also responsible for crisis management and critical infrastructure protection processes in their countries. Considering the importance and complexity of these processes, the responsible team's maturity is one of the key factors determining success or failure.

This document focuses on the maturity of national and governmental Computer Security and Incident Response Teams (CSIRTs) and the Trusted Introducer[1] certification scheme for CSIRTs as an indicator of the maturity level of teams. The issues covered are described from two points of view: the perspective of the team that is preparing for the certification process on the one hand and of teams that have already undergone certification and even recertification on the other. The aim of this document is to be a guiding tool for those national and governmental CSIRTs which are considering reaching the next level of maturity and good understanding of their capabilities.

This document gives recommendations for CSIRTs on how to improve and mature and be better prepared to protect their constituencies.

ENISA has carried out a considerable amount of work in this area, and this document contributes by sharping the role of ENISA in helping national and governmental CSIRTs on their way to a higher maturity level.

The motivation for national and governmental CSIRTs to gain certification is usually:

- Public Relation reasons – locally (towards the supervising institutions) and internationally (to show the 'level of the country');
- to evaluate CSIRT organisation against international criteria;
- an external drive to understand, document and put in order processes within the CSIRT team;

[1] https://www.trusted-introducer.org/

- to establish or put in order auditing, accountability and reporting schemes;
- to implement continuous improvement in a quality management framework.

Teams seeking certification can be classified into three categories:

1. Teams seeking to demonstrate maturity as proof of the team's experience and status (in this case certification can help teams to identify aspects of their operation that they have not considered).

2. Teams looking for external stocktaking of the team's capabilities (for example new teams that need a clear baseline of their own capabilities).

3. Teams in need of compliance according to governmental requirements. This is especially challenging when a team is new and governmental pressure is high. In those cases, it can be very challenging and resource consuming to implement all necessary changes within a given timeframe.

Nowadays the role and functions of countries' national and governmental CSIRTs are expanding and growing, so teams must keep up with newly created demands and expectations. Improving maturity allows teams to constantly enhance their capabilities.

This document should serve as a guidance tool for all, but especially national and governmental CSIRTs that are aiming to advance their maturity in all aspects related to CSIRT work. The combination of honest feedback about the certification process from already certified teams, as well as from a team in the process of getting ready for certification, together with ENISA's experience is a practical help for all teams considering advancement and certification.

1. Introduction

1.1 Aim of this document

This document aims to be a guiding tool for national and governmental CSIRTs which are considering to improve their maturity and potentially being certified (e.g. through Trusted Introducer[2] certification). The document builds on several previously published ENISA documents:

- CERT community – Recognition mechanisms and schemes[3];
- Deployment of Baseline Capabilities of n/g CERTs – Status Report 2012[4];
- Other documents related to baseline capabilities[5].

Additionally this study takes account of the 'CSIRT Maturity Kit – A step-by-step guide towards enhancing CSIRT Maturity' that was developed by NCSC-NL in The Netherlands[6] .

SIM3[7] (Security Incident Management Maturity Model) is a tool to assess incident management capability and maturity. Drafted by Don Stikvoort and Klaus-Peter Kossakowski, it has been adopted by the TF-CSIRT/TI community for its certification scheme. This study provides information on standing and issues regarding each SIM3 parameter and it includes case studies (for example the case of CERT.LV, the Latvian national CISRT that at the time of writing is preparing for the TI certification process). Finally, we include advice from already certified national and governmental CSIRTs from the Netherlands, Finland, Sweden and Switzerland, and other kinds of comments and advice from the Trusted Introducer team. ENISA is an important partner for national and governmental CSIRTs on their way to enhanced maturity; this document also outlines how ENISA contributes to this process and how it can be of assistance to an interested team.

Previously published ENISA documents on CSIRT baseline capabilities divided all related parameters into four categories: mandate and strategy, service portfolio, operation, and cooperation. These categories are not directly in line with the SIM3 model though they closely represent the group of capabilities. Since the SIM3 model is used for the Trusted Introducer certification, this document focuses on all parameters based on this classification.

1.2 Target audience – National and governmental CSIRTs

The target audience of this document are CSIRTs that either want to assess their current level of capabilities by an existing CSIRT evaluation scheme or need to advance their maturity level for various reasons. In particular, national and governmental CSIRTs in the European Union (EU), European Economic Area (EEA) as well as other neighbouring countries are the main target audience for this document. The Trusted Introducer certification scheme is available worldwide and does not set any geographical limitations for teams to become certified. However, TF-CSIRT (the GÉANT task force for security incident response teams), which

[2] https://www.trusted-introducer.org/
[3] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes
[4] http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012
[5] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities
[6] https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf
[7] https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

runs the Trusted Introducer certification, has defined that its geographical scope is aligned with the RIPE NCC service area[8].

(In general: the Trusted Introducer certification is suitable for any types of team but there are specific characteristics to be taken into account for national and governmental CSIRTs. Considering the fact, that ENISA's main stakeholders are national and governmental CSIRTs we focus on this group, and the "real-life examples" included in this document are taken only from national and governmental CSIRTs, Trusted Introducer experts and ENISA's experience in this area.)

Considering the current political and economic trends in Europe as well as the importance of networks and systems the EU economies, Member States need to plan ahead in order to protect their digital assets. The EU Network and Information Security Directive[9] (proposed by the Commission in 2013 and currently in the final stages of negotiations between the European Parliament and the Council) aims at ensuring a high common level of cybersecurity, including "the setting up of […] efficiently functioning CSIRTs" and "establishing a cooperation network among them".

[9] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Brussels, 7.2.2013, COM(2013) 48 final, 2013/0027 (COD), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666

2. CSIRT Maturity

2.1 CSIRT development pattern

The most thorough document on the CSIRT development pattern published so far in the EU is the ENISA deliverable 'CERT community - Recognition mechanisms and schemes'[10]. This document builds on information provided by the community and ENISA's experts, and it emphasises issues and gaps specific to capabilities of national and governmental CSIRTs.

The national and governmental CSIRT development process usually varies from country to country. Some countries begin with defining a national cyber security strategy, following later with appropriate legislation and the establishment of a CSIRT. Other countries start with the establishment of a CSIRT and the legislative basis and strategies follow later. Whatever the process, it is very important for a national and governmental CSIRT to have a clear mandate and a clearly defined constituency as soon as possible. The provision of basic services (in most cases the first one would be incident response) marks the real establishment of the team.

When international collaboration begins and the team recognises the need for international contacts and information exchange, the first steps in the international recognition process is taken. The Trusted Introducer scheme is widely used in Europe for this purpose. It offers three levels:

- Listing – the team is operational and contact information is available to other teams.
- Accreditation – the team is fully functional, services are defined according to RFC2350[11], etc. The team's information needs to be updated every four months, which lies in the responsibility of the team itself.
- Certification – the team has reached an appropriate level of maturity. (Certification is discussed in more detail in the following chapters.)

2.2 Maturity models

The maturity of an organisation is defined as measurement of its capability in terms of structure, people, processes and technologies. It provides a certain level of assurance that the organisation can perform its activities and functions consistently and is trustworthy, as well as being able to focus on constant development.

In the case of national and governmental CSIRTs, maturity assesses a teams' ability to manage (document, perform and measure) CSIRT capabilities and services in particular.

Historically, many national and governmental CSIRTs have developed from very informal, sometimes ad hoc groups of highly skilled and motivated people. Given the growing amount of tasks and responsibilities, there is a need for an adequate level of organisation and governance. There needs to be thorough understanding about CSIRT internal processes that ensures consistency in the provision of services and a clear pattern of development and improvement of the team's capabilities.

[10] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes
[11] https://www.ietf.org/rfc/rfc2350.txt

There are several maturity models in place. As mentioned this document mostly focuses on the SIM3 model which was developed in 2010 by S-CURE and PRESECURE with the help of the TF-CSIRT community. This model is the basis for the Trusted Introducer certification process described in detail later.

In 2015, the National Cyber Security Centre of the Netherlands published a document, 'CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity', which provides good practices for CSIRTs to achieve a higher level of maturity. This document is of rather general nature and does not target the national and governmental CSIRTs in particular, but is valid for any kind of CSIRTs. The toolkit is accompanied by an online tool to support teams to assess their maturity. The CSIRT Maturity Kit[12] provides a set of questions that to be considered (i.e. "What steps are taken to perform a certain service?", "Are these steps properly documented?", "What are the different roles of the team members?", "Are these well-defined?" How is performance measured?" and "Is this measurement redone regularly?").

Other, non-CSIRT centric certification schemes exist on the market as well. Best known are those related to international standards, for example, ISO 27001. Those are very well established schemes but are best suited to large organisations rather than to specific, security incident oriented teams such as CSIRTs. Few CSIRTs have gained certification based on ISO 27001, and most of the teams in Europe feel that this scheme is not particularly suited to them.

In addition, there are frameworks such as Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) available for IT environments and services. While they are targeted at organisations of any size, they might be considered too complex to implement in most national and governmental CSIRTs.

2.3 TI certification

The Trusted Introducer (TI) certification process is described in detail on the Trusted Introducer website[13].

To consider certification, the team has to be a "Trusted Introducer accredited team". TI certification is targeted at those TI accredited teams who have internal and/or external reasons to have their maturity level verified in an independent way.

A candidate for TI certification is a team that is already TI accredited in good standing – i.e. fulfilling their accreditation obligations for at least eight months and not being under special review by the TF-CSIRT Steering Committee – and has attended at least one of the TI meetings, which are co-located with the TF-CSIRT meetings three times a year.

The scheme used for measurement is the SIM3 model, describing 45 parameters, divided in four categories:

- Organisation
- Human
- Tools
- Processes

Scoring for each category is on five levels, ranging from '0', which means the parameter is not taken into account, to '4', which means that the parameter is not only described – as on level '2' – and rubber-stamped

[12] https://check.ncsc.nl
[13] https://www.trusted-introducer.org/

– as on level '3' – but is also part of an internal or external audit process. The actual certification gauging involves specific and distinct minimum levels for each of the parameters.

Examples of implementation of the five levels:

- 0 – not available in any form;
- 1 – the team is aware of this issue and has some way of dealing with it, but it is not documented;
- 2 – the topic is documented, for example, in an internal wiki or in a handbook;
- 3 – the topic is documented and approved by the head of the CSIRT, for example, an approved handbook, signed documents, etc.;
- 4 – the parameter is audited, there is active feedback from the auditors or upper management, for example external audit reports, actively approved quarterly or yearly reports, etc.

Once certification level is reached, the certified teams remain part of the community of TI accredited teams; the certification is an extra branding, useful for all sorts of purposes in the team's future.

TI certification can take from three to twelve months, depending on the amount of work the team needs to do to meet the requirements, and depending on the priority attached to that improvement process. The certification stays valid for three years, after which time the team needs to go through the recertification process to prove that the level of quality is maintained or even improved.

As of September 2015, fifteen teams have been certified, five of them are already recertified after the initial three-year period, two more are currently in the process of recertification and another three accredited teams are currently certification candidates[14].

[14] https://www.trusted-introducer.org/directory/alpha_certification_Z.html

3. Certification Process

The following description of the certification process is mostly based on information provided by the Trusted Introducer experts who are authors of the SIM3 model, and are currently carrying out certification workshops with teams that are certification candidates.

3.1 Certification

The first step at the outset is to understand the team's motivation behind certification. (See the Executive summary for typical motives for national and governmental CSIRTs.) Motivation might influence the priority of the process and resources, which can be allocated to improve the team's procedures and documentation.

The next step for any team considering certification is to make a self-assessment using the SIM3 model. The result will provide the first indication of how many of the requirements are already in place and which areas are lagging behind.

Understanding the scaling (0/1/2/3/4) for the SIM3 model is very important for achieving correct self-assessment results. When in doubt consultation with the Trusted Introducer experts to align the understanding is needed (see chapter 2.3 for some examples of rating).

Another step in preparation for the certification is to collect reference materials and documentation, for example mandate and regulation, constituents, etc.

Some national and governmental CSIRTs have mostly a coordinating role. For those some of the parameters are not applicable, in which case they are excluded from the evaluation and get a score of '-1'. The goals of purely coordinating teams are different from those of operational teams and this is also respected during the evaluation process.

3.1.1 Language

Trusted Introducer team members speak several different languages (English, German, Dutch, Polish, Russian and French) but it might well happen that the CSIRT operates in a language, which is not known to any of the TI experts.

Usually if the team is a member of FIRST and a Trusted Introducer accredited team they have some documentation in English (at least the RFC2350 document). Trusted Introducer experts do not ask for official translation of the documentation because it would be very expensive and time-consuming. TI tries to engage a native language speaker (who is not a member of that particular CSIRT) to validate whether TI's understanding of certain criteria corresponds to documents in the native language.

Some CSIRT internal documents can be translated quite easily (for example workflows) using translation tools, if confidentiality permits. Translation of complex and long documents or documents with confidential information is usually not required. However, teams have to ensure that enough information is provided to the TI experts to enable them to understand and verify the real situation.

The certification process is accompanied by a workshop (see next chapter), where the open issues can be discussed. The protocol of the workshop has to be signed by the team leader, confirming those points, which could not be verified because of language issues.

3.1.2 Certification workshop

A certification workshop is a full-day event taking place at a team's premises. The requirement is that at least three CSIRT members participate. The team's processes, procedures and tools are discussed, and different team members are asked to express their opinion to ensure that there are no significant internal differences in understanding the way the CSIRT works.

The main goal of the workshop is to help the team to identify areas which are lacking either documentation or procedures and to improve them. (Experience shows that every team has something to improve; no team has just sailed through the certification!)

3.2 Re-certification

According to the Trusted Introducer's process, a team's certification is valid for three years. Thereafter, the team has to go through the recertification process in order to keep the certification valid.

The main goal of the recertification process is to discuss how the team has advanced their maturity during last three years. If no advancement has taken place, the recertification is endangered because the team has spent three years being static and has expended their efforts on something else.

Certainly, there are cases in which no advancement should be expected. For example, if a team has moved from one hosting organisation to another or the mandate has been extended, the team will have spent most of its resources adapting to the changes and different expectations. In such cases, the recertification might not be endangered due to a lack of progress but to missing or still to be adopted changes.

Therefore, if no advancement can be determined, a clear understanding of the root causes must be gathered during the recertification workshop. In case extensive organisational changes have occurred, the compliance of all factors needs to be carefully considered, in that case, not for any expected improvements but mostly how the past status quo was maintained.

During the recertification, the workshop assessment report from the previous (certification) workshop is discussed and the team's status then and now is compared (also during the recertification process a workshop is held, but it is usually half-day instead of full day).

4. Maturity of Organisational Parameters

In the following chapters the parameters of the SIM3 model are discussed. For each parameter the minimum level for the certification is indicated after the title. General explanations and suggestions are given, accompanied by examples from the case study for CERT.LV and comments from four certified national and governmental CSIRTs. General suggestions are given at the end of each parameter's chapter.

4.1 O-1.Mandate

4.1.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

In the case of national and governmental CSIRTs, there is a strong requirement for a legislative document (however, this is not required for achieving the certification, but considered good practice) or other mechanism clearly setting out the mandate of the CSIRT. As previously emphasised by ENISA studies, ***The mandate, especially the definition of roles and responsibilities, needs to be clear enough to support all relevant activities of the*** [15]***national and governmental CSIRT***. The mandate of national and governmental CSIRTs needs to be publicly announced. The mandate should also be available in English. ***Special provisions (e.g. funding) need to be included in the mandate for the national and governmental CSIRT-type roles and functions.***[16]

The mandate is a basic requirement for any CSIRT, but for national and governmental CSIRTs ENISA calls for a strong legal basis for their operations.

The mandate should also include the accountability of the national and governmental CSIRT to a higher/governing body (e.g. a ministry or regulatory body).

4.1.2 CERT.LV experience

CERT.LV is the national and governmental CSIRT of Latvia. The main governing document of CERT.LV is the Law on the Security of Information Technologies[17] (hereafter referred to as 'the law'). It states that the activities of the IT Security Incidents Response Institution shall be ensured by the leading State administrative institution in the national defence sector (i.e. Ministry of Defence), which delegates functions of CERT.LV to the Institute of Mathematics and Informatics, University of Latvia. This CSIRT has been established by Law. In many cases, the hosting organisation would be determined by a concluding agreement. In addition, the law states that functions and tasks should be fulfilled according to the delegation

[15] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 (here and after identified gaps are quoted with relevant chapter - chapter 5.2 Mandate)
[16] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 5.2 Mandate
[17] Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:
1 November 2012; 6 November 2013; Law On the Security of Information Technologies;
http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.doc

agreement (that is renewed annually) and provides a set of conditions for CERT.LV. Existing framework (the law) provides a clear mandate as well as defines tasks, responsibilities and accountability for CERT.LV.

4.1.3 Comments from certified teams

For all certified national and governmental teams, organisational parameters seem to be straightforward. The mandate in most cases is clearly set in a law and later in corresponding national legislation. Only one team mentioned that their functions actually exceeded the mandate, so a change of legislation was needed and this situation has been resolved for the recertification.

4.2 O-2.Constituency

4.2.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

National and governmental CSIRTs have different constituencies and sometimes both roles are combined in one team. The usual constituency of a governmental CSIRT, therefore, is usually the government and other public bodies. National CSIRTs on the other hand have responsibility for an economy or a country[18], they can act as the national point of contact (PoC) for information sharing (such as incident reports, vulnerability information etc.) with other national CSIRTs in the EU Member States and worldwide. Sometimes national CSIRTs are the last resort CSIRTs for everybody within a specific country, but sometimes, especially for small countries, their constituency is the whole country including the public sector, the private sector, end-users, etc.

For a national and governmental CSIRT, the constituency has to be clearly defined in legislative documents (it is not required for minimal certification, but considered best practice) or set out with a similar high level mechanism. The description of the constituency has to be publicly available (also in English). The definition of the constituency is a basic requirement for any CSIRT, but for national and governmental CSIRTs ENISA calls for a strong legal basis for its definition.

4.2.2 CERT.LV experience

CERT.LV is the governmental and national CSIRT of Latvia in the broadest possible sense, with the mission of "promoting IT security in Latvia". For practical purposes, CERT.LV's constituency is defined as IP addresses hosted in Latvia and all resources within the TLD.lv. The law defines certain responsibilities towards different groups of constituency (state institutions and municipalities, IT critical infrastructure owners, ISPs), but CERT.LV offers some services (depending on resource availability) to anybody in Latvia.

4.2.3 Comments from certified teams

The constituency of certified national and governmental CSIRTs was in most cases defined in a regulation. Two of the teams have additional agreements in place with some constituents.

[18] https://www.cert.org/incident-management/national-csirts/national-csirts.cfm

4.3 O-3.Authority

4.3.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

The authority of national and governmental CSIRTs has to be clearly described – i.e. what they are allowed to do towards their constituency in order to achieve their goals. It is very beneficial if authority is defined in legislative documents (this is not required for minimal certification, but considered best practice). The description of authority has to be publicly available (also in English). For national and governmental CSIRTs ENISA calls for a strong legal basis for their authority.

To allow CSIRTs to carry out their tasks it is important to give them sufficient authority/rights. The following areas should be taken into consideration:

- private data processing (especially when related to data involved in an incident);
- rights to demand cooperation and information from operators/ISPs;
- rights to demand cooperation and information with/from governmental sectors;
- rights towards Critical Information Infrastructure holders (owners or operators).

4.3.2 CERT.LV experience

The legal framework of CERT.LV includes the Law on the Security of Information Technologies, several specific laws and corresponding rules of the Cabinet of Ministers (including Regulations regarding "the Information to be Included in the Action Plan of a Merchant of Electronic Communications, the control of the implementation of such plan and the procedures, by which end users shall be temporarily disconnected from the electronic communications network[19] and procedures for the planning and implementation of security measures for the Critical Infrastructure of Information Technologies"[20]). Overall authority and legal rights are explicitly defined in this framework. Main rights of CERT.LV include the right to receive information about incidents (mandatory requirement to inform CERT.LV about incidents for certain groups of constituency), process data streams (based on mutual agreement with target institutions), carry out penetration testing of defined infrastructures, and request a disconnect of end-users for a time up to 24 hours.

In addition to the authority defined in the legal framework, CERT.LV is continuously working on cooperation and awareness raising within the constituency, which is beneficial in everyday activities and improves the visibility of CERT.LV among different actors in the IT security field.

[19] http://www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._327_-_Action_Plan_of_a_Merchant_of_Electronic_Communications.doc

[20] http://www.vvc.gov.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._100_-_Planning_and_Implementation_of_Security_Measures.doc

4.3.3 Comments from certified teams

The authority is (or will be) described in the law and corresponding regulations, two teams describe authority additionally in agreements with constituents.

4.4 O-4.Responsibility

4.4.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Minimal certification requirements do not require responsibility to be defined and actively audited in documentation provided at the level beyond CSIRT management, though in the case of a national and governmental CSIRT clear description of responsibility in legislative documents would be an advantage to everyday CSIRT activities. Regardless of its legal status (outside approved or just by the CSIRT manager), a clear description of CSIRT responsibility should be publicly available (also in English).

If a national and governmental CSIRT carries out its tasks, there might be a tendency to assign the CSIRT with new functions which could be different from CSIRT core functions (for example, when a new function is needed because of a new legislative document). Fulfilling new tasks might be challenging unless appropriate new funding is provided. It should also be checked carefully whether new tasks are not conflicting logically with CSIRT core functions. For example a CSIRT cannot fulfil the same function which it has to supervise.

Clear description of responsibilities and understanding in the fields of Critical infrastructure protection and cooperation with law enforcement are needed. ***Cooperation with law enforcement authorities can be one-sided, in cases where LEAs are not in a position to share information, particularly during an investigation. While certain legal barriers need to be respected, there are ways that national and governmental CSIRTs can keep lines of communication open and work together in areas of mutual interest.***[21]

4.4.2 CERT.LV experience

Responsibility of CERT.LV is clearly defined in the legal framework.

Thanks to the improved visibility (especially) within governmental institutions, CERT.LV gets additional responsibilities when new functions related to IT security need to be assigned. Sometimes these new functions are temporary until the responsible institution is established (e.g. in the planned NIS directive framework). Additional functions do not always have appropriate funding and have to be performed using existing work force. Another issue with additional functions is that they can conflict with current CERT.LV activities. An institution should not be auditing a process when it is directly involved in that process – for example, CERT.LV cannot support a governmental institution in solving incidents at the same time as auditing incident handling.

[21] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 8.1 National Cooperation

4.4.3 Comments from certified teams

Responsibility of the certified national and governmental CSIRTs in the best-case scenario is described in a law. If the responsibility is not clear, there are agreements in place with the constituents. In one case the team pointed out that the agreement had been general, allowing quick adaptation to the changing situation and emerging threats.

4.5 O-5.Service Description

4.5.1 Requirements

MINMUM LEVEL	DESCRIPTION
4	Explicit, audited on authority of governance levels above CSIRT head – subject to outside control/audit

Service description has the highest certification requirement; it needs to be actively audited at one level above the CSIRT management. That requires contact information, a description of CSIRT services (also in English) and the CSIRT policy on information handling and disclosure (all of which are publicly available), and in the case of national and governmental CSIRTs, a clear description of services in legislative documents.

If there is a service description in a legislative document it might be the case that only basic (usual) services are stated and ***CSIRTs do not offer services beyond the usual portfolio which might bring additional benefits to their constituents.*** Also the opposite might be the case: ***there may be services provided by the national and governmental CSIRTs that are not considered as added value by the constituents, or may also be provided by other CSIRTs or commercial vendors.***[22]

Regarding additional services – as discussed in the baseline document – ***vulnerability and artefact handling are not fully provided by all CSIRTs***[23] and the ***majority of national and governmental CSIRTs are still not involved in disaster recovery planning and business continuity management.***[24]

4.5.2 CERT.LV experience

As stated in the law, all services of CERT.LV are provided without additional charge and cover the usual portfolio of CSIRT services:

- reactive services, i.e. services that are initiated by an incident (such as support and coordination of incident handling);
- proactive services, i.e. services that try to prevent incidents (such as recommendations on mitigating security risks, penetration testing);
- Awareness-raising services, i.e. provision of information and distribution of educational materials in order to raise awareness about computer security issues to reduce the number of incidents.

[22] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 6.2 Proactive Services
[23] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 6.3 Reactive Services
[24] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 6.4 Security Quality Management Services

The basic set of responsibilities is defined by the law – CERT.LV:

- maintains common electronic information space monitoring;
- provides support in information technology (IT) security incident prevention or coordinates their prevention;
- maintains in a publicly accessible way, in line with the actual threats, recommendations on the current IT risks;
- conducts research, and organises educational events, education and training in the field of IT security;
- provides support to state institutions in safeguarding national security, as well as crime and other crime detection (investigation) in the field of IT, complying with statutory restrictions on data processing;
- monitors state and local governmental institutions and telecommunication operators' compliance with the duties prescribed by this law;
- cooperates with internationally recognised IT security incident prevention institutions (teams);
- carries out other obligations under laws and regulations.

Additional services include certification of systems for collecting signatures both for the European Citizens' Initiative and for national legislative initiatives, as well as development of best practice documents of the IT security framework (policies, risk assessment, recovery planning etc.) for state institutions and local municipalities.

4.5.3 Comments from certified teams

Service description in the case of one team has been quoted in the respective regulation; others set it out in the agreements with the constituency or in the RFC2350 document. In one case, the team mentioned that some services (for example, information sharing) are provided without particular documentation but "because constituents need them".

4.6 O-7.Service Level Description

4.6.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Service level description with regard to minimal certification requirements contains the need for specification of reaction time to incoming incident reports as well as minimum human reaction for reports from peer CSIRTs (recommended within two working days). As general principle a national and governmental CSIRTs should be reachable 24/7.

Although the national and governmental CSIRTs now provide or are shortly to provide 24/7 operational mode, this crucial facility is not always properly displayed on national and governmental CSIRTs' website.[25]

Since full deployment of 24/7 is very expensive and it is difficult to get qualified technical experts to work in shifts, some "semi-24/7" options should be considered:

- outsourcing of the CSIRTs hotline with clear instructions of what to do in any particular case (which incidents can wait until the next working day and which have to be escalated immediately);
- distribution of CSIRT core employees' mobile phone numbers to all major partners including peer CSIRTs (for example, via the Trusted Introducer database);
- the person on duty within the CSIRT to be contacted if the situation has to be escalated by the call centre.

4.6.2 CERT.LV experience

CERT.LV is authorised to address all types of current or upcoming computer security incidents in all networks in Latvia.

The level of support given by CERT.LV will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CERT.LV's resources at the time; though in all cases some response are made available within one working day. The service level is defined in the internal CERT.LV documents.

4.6.3 Comments from certified teams

Service level description in the case of one team has been drafted in the regulation; others set it out in agreements with the constituency or in the RFC2350 document. Service level might be different for different types of constituency. The level itself ranges from best effort to clearly defined parameters.

4.7 O-8.Incident Classification

4.7.1 Requirements

MINMUM LEVEL	DESCRIPTION
1	Implicit – awareness, knowledge in head, experience

The minimal certification requirement is to be aware of incident classification. However, as classification is the basis for the incident handling and reporting process, some kind of description is needed. There is no unified classification scheme for CSIRTs, which means ***there are differences in terminology and schemes applied by national and governmental CSIRTs***[26]***.*** In addition, incidents are not clearly distinguishable – there might be combined types of incident and new kinds of incident that do not fit into the existing classification.

[25] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 - chapter 7.1 Human resources

[26] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 8.3 Best Practices for Cooperation

There are several examples that can be used as a basis for CSIRT incident classification (see the ENISA web page[27]).

Each CSIRT should choose a scheme to classify incidents which best fits its needs, taking into account incidents with which they are dealing, statistics process, requirements of the constituency, legal requirements of the country where appropriate, etc.

4.7.2 CERT.LV experience

CERT.LV divides all incidents into high and low priority incidents. High priority incidents are reported individually (no automatic reporting) or those that concern high risk institutions (government, critical infrastructure, etc). Low priority incidents are all those which are automatically reported by CERT.LV partners (infections, IPs in botnets, misconfigured devices, etc) and do not concern high risk institutions. Priority determines the incident resolution process; incidents assigned high priority are handled individually while low priority ones are handled in a fully automated manner.

CERT.LV has defined the following high priority incident categories (available on line in Latvian and English[28]):

- **Compromised Asset** – Unauthorised access to the servers / network equipment / IT systems / applications / user accounts;
- **Denial of service** – Denial of service (DoS) or distributed denial of service (DDoS) attack;
- **Phishing** – Attempts to acquire information such as usernames, passwords, and payment card details by masquerading as a trustworthy entity;
- **Hacking** – Reconnaissance or suspicious activity originating from outside the network device. Automatic attacks in order to find usernames and passwords. Targeted attacks to find vulnerabilities;
- **Spam** – Any kind of spaming, including the generation of spam;
- **Malware** – Malicious code distribution;
- **Botnet** – Infected device which can execute commands from a botnet centre;
- **Other** – Virus infection, consulting, theft, fraud, child pornography, copyright, personal data.

The classification scheme is revised and updated when needed.

Each category has a priority assigned, which together with the priority of the affected institution forms the basis for incident triage and handling.

4.7.3 Comments from certified teams

Certified teams generally did not mention any issues with the classification. One team mentioned that its classification is based on the eCSIRT.net[29] model. Most of the certified teams have implemented a classification in the ticketing system or other tools. One team is currently working on a more detailed model for incident classification due to the changes in legislation that will introduce mandatory incident reporting in the country.

[27] https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies
[28] https://cert.lv/section/show/91
[29] http://www.ecsirt.net/

4.8 O-9.Participation in existing CSIRT Frameworks

4.8.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

National and governmental CSIRTs usually have no upstream CSIRT. In cases where more than one national and governmental CSIRT exist in a country there might be an issue with cooperation and with a clear definition of the "National point of contact" for teams of other countries.

If a team is considering certification it means it is participating in at least the Trusted Introducer framework (and after certification it needs to be present in at least three out of nine Trusted Introducer meetings). Many teams face problems with resources (both human and financial ones) to allow them to participate in several *fora*. Nonetheless, for national or governmental teams it is important to represent the country of origin (as national single PoC for other CSIRTs), build relationships with other teams and exchange information. The EU CSIRT network of the proposed NIS Directive[30] is foreseen as a suitable mechanism to address this lack of resources.

National and governmental CSIRTs should also think about forming special relations with CSIRTs of neighbouring countries. This might include different types of cooperation, from informal personal contacts to a more formal Memorandum of Understanding, technical information sharing, usage of common secure chat systems (e.g. Jabber) and others. The issue of trust is crucial in all CSIRT partnerships, including international cooperation, and an obvious observation is that trust is difficult to build and even more difficult to maintain.

The national and governmental CSIRTs in the EU have reached varying levels of maturity, which may be detrimental to more effective cooperation.[31]

When handling incidents internationally, partnering national and governmental CSIRTs sometimes do not act as expected upon information provided. There can be a number of reasons for this. In some cases, this could be due to the lack of a standardised framework for information exchanged, which makes it difficult for national

[30] The proposed NIS Directive (European Commission, 2013a) is now undergoing the final stage of negotiations between the EU legislative bodies; it is hoped that it will be adopted shortly (Latvian Presidency of the Council of the European Union, n.d.). As recently reported, the "EU Digital Commissioner Günther Oettinger said […] [on 9 November 2015] that an agreement on new, long-awaited cybersecurity legislation is only "days or weeks" away. European Commission, Parliament and Council officials are about to sign off on a compromise deal on the network and security information (NIS) directive, according to Oettinger. […] Luxembourg, the current holder of the 6-month rotating Council presidency, is now trying to push through an agreement in the last weeks before its term ends on 31 December." (Stupp, 2015). To follow the status of the procedure, including proposed amendment to the proposal, see: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027(COD)#basicInformation (last access date: 14 November 2015)

[31] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 8.3 Best Practices for Cooperation

and governmental CSIRTs to analyse and identify the relevance thereof. But there are other factors like in some cases legal/data protection barriers or limitations to act ultra vires beyond a specific delegation of powers..[32]

4.8.2 CERT.LV experience

CERT.LV has been a full member of FIRST since April 2009 and a Trusted Introducer accredited team since 2008. (Although CERT.LV was formally established only in 2011, it developed out of CERT NIC.LV and LATNET CERT, which were both established already in 2006.) CERT.LV also participates in the Annual Meetings for CSIRTs with National Responsibility organised by CERT.CC and in the activities for national CSIRTs organised by ENISA.

On a case-by-case basis, CERT.LV negotiates bilateral partnership, for example, by a Memorandum of Understanding.

4.8.3 Comments from certified teams

All certified teams actively participate in the existing CSIRT frameworks such as FIRST and TF-CSIRT/Trusted Introducer. Most of them have at least one responsible/contact person for every contact network/organisation. From a certification point of view, this parameter can easily be proven by the respective organisation (for example through listing in the database of FIRST members, etc). In general, teams stressed the importance of participation in these frameworks.

4.9 O-10.Organisational Framework

4.9.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

A clear organisational framework document is needed not only for certification, but also it should be available and usable for team members. This document should describe not only the above-mentioned organisational parameters but also the organisational structure of a CSIRT as well as the CSIRT's place in the national IT security framework. There might be supporting documents/reference documents that, depending on the level of classification, should be available to all CSIRT employees.

The description of the organisational framework can be done in a single document like a handbook, or the information can be collected in an internal wiki. Other solutions are possible as well.

4.9.2 CERT.LV experience

CERT.LV has a document called 'CERT.LV Handbook' which serves both as a main document for the organisational framework and as a set of procedures and normative documents and references in order to formalise knowledge that exists mainly in team members' heads. This document also increases reassurance within the team and improves the awareness of new employees.

[32] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 6.1 National/governmental CERT Core Services Capabilities

4.9.3 Comments from certified teams

This is one of the parameters where certified teams have different approaches. All of them have a RFC2350 document in place but some teams have used the certification process to develop a more formal and broad 'umbrella' document/ handbook. Teams that have handbooks or wikis stressed that they are updated and actively used.

4.10 O-11.Security Policy

4.10.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

Obviously, a CSIRT as an organisation also needs a security policy for its own purposes. The policy might be part of the host organisation's security policy, if different. From the CSIRT perspective, primarily this policy should focus on the protection of sensitive information i.e. confidentiality. When writing the security policy, local legislation must be taken into account, especially relating to personal data protection and information classification and protection. CSIRTs might consider developing a policy that is compliant with international standards (for example ISO 27001).

4.10.2 CERT.LV experience

CERT.LV has adopted a security policy based on the ISO 27001[33] framework, taking into account some local legislative requirements. The work on the CERT.LV security policy allows CERT.LV experts to gain experience in order to develop best practice documents (policies, risk assessment, recovery planning, etc.) for state institutions and local municipalities.

4.10.3 Comments from certified teams

All teams have the security policy of the hosting organisation in place (in one case the host organisation is ISO 27001 certified, so the policy is part of that). Some of the teams have participated in developing the policy. However, most of the teams have some additions and specific guidelines to that policy relating to CSIRT activities, including, for example, TLP[34] usage.

4.11 General comments on organisational parameters

According to the Trusted Introducer experts' feedback, organisational parameters for national and governmental CSIRTs are usually in very good shape, fully documented and seldom raise any serious issues.

Although the certified national and governmental CSIRTs did not mention any issues with incident classification, TI experts reported that issues sometimes arise, for example, when the classification is not aligned, it is not well communicated to the constituency, or it is not supported by automated tools. The main question arising during the certification is whether the incident classification is suitable and the team is comfortable with it.

[33] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[34] https://www.trusted-introducer.org/ISTLPv11.pdf

As an example, in Germany there are certain legal requirements regarding the classification of incidents and reporting requirements, but that classification might not be the best one for the organisation to gain situational awareness, so the internal classification must be tailored to the reporting requirements by law.

During the certification process, a Trusted Introducer expert does not evaluate differences between different teams' classification because although there are usually similarities between teams, some parts always differ. For example, classification might be determined by the tools used or promoted by local government. There is no consistent way of classifying incidents in Europe and this is one of the future directions for possible harmonisation.

Teams should consider using the O-10 parameter to write a document that covers many other parameters in terms of documentation. This can either be a separate document – a handbook, charter or organisational framework – or information can be gathered in the team's wiki.

5. Maturity of Human Parameters

5.1 H-1.Code of Conduct/Practice/Ethics

5.1.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Certification requires a certain set of rules or guidelines for CSIRT members for professional behaviour both within and outside work. The CSIRT Code of Practice (CCoP)[35] is provided by the TF-CSIRT community as an example. The CCoP covers legal requirements (including when dealing with incidents outside the particular CSIRT's country), being responsible when sharing information, as well as some specific requirements in cases of vulnerability research. In the case of national and governmental CSIRTs, certain behaviour should be expected from CSIRT employees, especially when dealing with outside partners. However, a code of conduct/practice/ethics should not limit or disturb the normal working process of a CSIRT.

National and governmental CSIRTs can be part of a government and subject to the host organisation's code of conduct/practice/ethics (e.g. ministries) that might be too general for CSIRTs. In that case, requirements of the CCoP should be merged with the host organisation's requirements with due care.

All employees should be aware of the code of conduct and should be encouraged to discuss and constantly improve it.

5.1.2 CERT.LV experience

CERT.LV has adopted its own code of conduct and ethics. It includes requirements from the CCoP and from the host organisation's (Ministry of Defence) code of ethics. The document includes provisions on such topics as:

- legal requirements – focuses on the need to observe local legislation as well as take into account other countries' legislation if the particular incident 'crosses the borders';
- information exchange – responsible handling of sensitive information;
- avoiding a conflict of interest – specific provisions from the local legislation;
- professional behaviour – reasonable requirements for professional and respectful behaviour.

A draft code of ethics discussed in a team meeting and suggestions from the team members were taken into account.

5.1.3 Comments from certified teams

Most of the teams have some kind of code of conduct as part of the host organisation's policy and/or governmental requirements (such as rules for civil servants or as part of a security clearance process). One team mentioned that the code of conduct is one of the first things that are discussed with new employees.

[35] https://www.trusted-introducer.org/CCoPv21.pdf

On the other hand, one team relied more on a person's reputation within the community (before hiring) with no specific requirements for outside work behaviour.

5.2 H-2.Personnel Resilience

5.2.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Lack of qualified personnel is often one of the main issues for national and governmental CSIRTs. Certification requires that the team's minimum size is three (part-time or full-time) CSIRT members. It is quite common for CSIRTs to have part-time employees, though it should be clearly defined that in cases of emergency the work in the CSIRT should take priority over other working obligations.

As an extension to personnel resilience, it might be a good idea to have a group of volunteers as a back-up in case of a significant crisis. They should be involved in CSIRT exercises in order to have a basic understanding of CSIRT operations. In addition, security clearance issues should be taken into account.

Typically, CSIRTs are rather small, so a CSIRT should consider implementing procedures in order to ensure that each critical function has at least one primary and one back-up employee.

In special cases, a dedicated employee should be appointed (for example, on special/politically sensitive dates for 24/7 availability).

5.2.2 CERT.LV experience

CERT.LV ensures personnel resilience via the following:

- the staff is growing every year, reaching 15 FTEs in summer of 2015;
- flat structure – no division in departments and the shortest possible command chain;
- an outsourced helpdesk 24/7 with instructions on how and when to contact CERT.LV employees and basic information for simple cases;
- in the event of a significant crisis, CERT.LV has the potential to involve volunteers from the Cyber Defence unit which is part of the National Guards in Latvia; all members have security clearance and are trained to be able to participate in crisis mitigation. The Cyber Defence unit is always involved in the CERT.LV exercises.

5.2.3 Comments from certified teams

Teams did not point out any problems with personnel resilience, although not all of them provide a 24/7 service. Most of the teams have personnel resources available (for example, from the host organisation) that can be involved in the CSIRT operations in a case of crisis. One team also pointed out the importance of observing a healthy work/life balance for employees in cases of lengthy incidents. Depending on the functions and size of the constituency, national and governmental teams tend to have more than three employees. The size of national and governmental CSIRTs that are already certified varies between eight and 35 people in the core team and up to 100 employees in the host organisation which can be involved in CSIRT activities if needed.

5.3 H-3.Skillset Description

5.3.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

CSIRTs have members with different educational and employment backgrounds. Guidance materials on setting up a CSIRT include an overview of the skillset needed (for example, 'A Step by Step Approach on how to set up a CSIRT'[36] or the CERT Division of the Software Engineering Institute description on 'Operating and Staffing a CSIRT'[37]), so generally the skills needed for CSIRT operation are well documented.

The task of finding an experienced professional might be rather difficult, particularly for a national and governmental CSIRT (taking into account financial resources), so during job interviews CSIRTs should look for a person with the right mind set and attitude rather than expecting to hire a fully qualified professional.

Another dimension of a team's skillset is that the CSIRT should be aware of each existing member's skills and abilities (taking into account professional development) when complementing the team with new members.

The skillset should be defined internally by for example collect job descriptions in an internal wiki.

5.3.2 CERT.LV experience

Each position in CERT.LV has a description of duties, which is part of the employment contract. Requirements for each new position include a skillset description. Skillsets include incident handler, malware analyst, programmer, IT project manager, and IT auditor. When looking for new employees, CERT.LV takes into account existing skills within the team as well as skills required for the new or understaffed functions. These needs are matched with what is available in the job market and the best possible candidates are recruited, provided the salary CERT.LV can offer is acceptable, taking into account the global market situation.

5.3.3 Comments from certified teams

Skills needed for specific positions are described in the recruitment advertisements and job /function/ service description. Only one team maintains a separate skillset description besides that previously mentioned.

5.4 H-4.Internal Training

5.4.1 Requirements

[36] https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide
[37] http://www.cert.org/incident-management/csirt-development/resources-operating-staffing-csirt.cfm

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

Internal training should be used both to train new team members and to improve the skills and knowledge of existing ones.

For new employees, some kind of internal handbook (for example compiled during the preparation phase for certification) is useful in order to gain understanding of overall CSIRT standing. If possible, new members should make use of one (or more if possible) mentor – a more experienced team member who brings new member up to speed. Also an 'introduction round' would be advisable, during which the new employee becomes familiar with everybody and the functions of each team member.

CSIRTs should encourage internal information-sharing between employees and opportunities for professional development inside the CSIRT.

As national and governmental CSIRTs, depending on their situation, training related to security clearance (including information classification) is essential for new employees.

In any case, the procedure of mentoring and internal training should be documented to assist the team in this important and resource-demanding process.

5.4.2 CERT.LV experience

Each new employee for CERT.LV has a walkthrough/demonstration of the main CERT.LV tools (e.g. RTIR, internal customer database, etc.), an introduction within the organisation as well as specific briefings on information classification and sharing, safety issues and the code of ethics. Parts of these briefings are provided by the host organisation. Specific mentoring is conducted on a case-by-case basis. All CERT.LV educational activities are open to all employees. If the terms and conditions of external training allow, participants can share the knowledge and materials of that training internally.

There are informal internal presentations and educational activities as well as 'insecurity day' activities. The CERT.LV Handbook, besides documenting the internal training process, is also useful, along with the RFC2350 document, in providing an overview of CERT.LV activities.

5.4.3 Comments from certified teams

Teams mainly employ a mentoring process and an internal wiki to train new employees. Some of them have a more formal training programme covering all the basic aspects of the work (PGP, incident response system, tools, mandate etc.). Another approach is that internal training is a part of the host organisation's training policy.

5.5 H-5.External Technical Training

5.5.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

There is a number of possibilities for external technical training[38]. The challenge is to combine available needs and resources, while maintaining CSIRT operations during training. There should be mandatory external training for new members (for example, TRANSITS I[39]). It might be a good idea to make available online courses or webinars for gaining and maintaining the skills needed. TRANSITS II[40] is a more technical training that is useful as part of the staff's continuous education.

As national and governmental CSIRTs depend heavily on a fixed budget, it is very important to include training needs in the annual budget.

Teams should consider using ENISA's freely available trainings and "train the trainer program" for CSIRT specialists. National and governmental CSIRTs can ask ENISA to deliver specific training on an individual team basis.[41]

5.5.2 CERT.LV experience

A set of courses is mandatory for new team members (TRANSITS I, information security course from the Ministry of Defence). Participation in external training is organised individually according to the needs of employees and available resources. The budget for external training is planned each year, considering the profiles of employees and organisational limitations.

CERT.LV employees participate regularly in seminars and courses organised by ENISA and NATO CCDCoE[42], TRANSITS II events and, when possible, in external exercises.

Some of the team members have formal certificates in related fields, for example, Certified Ethical Hacker (CEH) and Certified Information System Auditor (CISA) certificates.

5.5.3 Comments from certified teams

Most of the teams mention TRANSITS I courses as a basic requirement for external training of new employees. Usually there is a well-documented process and budget available for external training. One team mentioned that the technical training required for CSIRT personnel is more expensive than the average budget for training civil servants from the host organisation. In that case, exceptions are introduced to allow for a different training type for more advanced skilled personnel.

5.6 H-6.External Communication Training

5.6.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

[38] https://www.enisa.europa.eu/activities/cert/training
[39] http://www.terena.org/activities/transits/transits-i/
[40] https://www.terena.org/activities/transits/transits-ii/
[41] https://www.enisa.europa.eu/activities/cert/training/want-to-know-more
[42] https://ccdcoe.org/

In national and governmental CSIRTs most team members deal with their constituency and peers on a regular basis. Mature CSIRTs should be capable of communicating efficiently with the press, media and society in general. At least some team members should receive advanced external communication training and basic training (perhaps internal or from the host organisation) should be considered for all team members.

The TRANSITS II course has an excellent basic communication module that is easily available to CSIRTs.

Subject to the availability of financial resources, national and governmental CSIRTs could consider recruiting crisis communications experts to deal with stakeholders and media.

5.6.2 CERT.LV experience

Although so far no specific communication training has been provided, it is planned. Some team members have participated in communication training as part of exercises and TRANSITS II courses.

There are three public relation specialists in the CERT.LV team who have a variety of experience in dealing with the media and public communication as well as the publishing of information. Most experienced CERT.LV team members have long experience in participating in radio and TV interviews, for which the necessary skills have been acquired through practice.

5.6.3 Comments from certified teams

Certified teams have different approaches on who is allowed to talk to media. In some teams, everybody can talk to media and therefore they all receive communication training. In other teams, only some employees can talk to the press, so communication training is not available to everybody. All teams mentioned, however, that they are considering the possibility of communication training for all team members.

5.7 H-7.External Networking

5.7.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

External networking has two components: going out and meeting other CSIRTs and more actively contributing to the CSIRT communities. There is a number of key organisations that allow CSIRTs to meet and communicate (e.g. FIRST, GÉANT (TERENA), ENISA). Opportunities occur more than once a year and in different locations, so national and governmental CSIRTs should find a way to participate in at least some of them.

National and governmental CSIRTs should be active in global forums (e.g. TF-CSIRT, FIRST), but, more importantly, they should participate in forums which are specifically created for them. Those are:

- ENISA-organised annual workshop 'CERTs in Europe'[43], which is dedicated to European national and governmental CSIRTs;
- CERT Coordination Center[44]-organised annual meeting of national CSIRTs;
- European Government CERT forum (EGC[45]) – a closed group of governmental CSIRTs.

Participation in external events is very important and an appropriate budget should be allocated annually.

5.7.2 CERT.LV experience

CERT.LV is a Trusted Introducer accredited team and a member of FIRST. Regular participation in TF-CSIRT, Trusted Introducer and FIRST events is agreed in the formal contract with the supervising institution.

Bilateral agreements and Memorandums of Understanding are negotiated and concluded on a case-by-case basis. These include cooperation with CSIRTs in other countries as well as with the commercial sector – security researchers, vendors and service providers.

The national and governmental CSIRT CERT.LV is open to cooperation with every stakeholder in the field of IT security.

5.7.3 Comments from certified teams

All teams stressed the importance of external networking. In most cases there is a dedicated contact person for every partner group (such as FIRST, EGC, TF-CSIRT, national groups). Meetings of that group are usually attended by the main contact person and another person from the team. For the second person, the rotation principle is used in some teams.

5.8 General comments on human parameters

According to the Trusted Introducer experts' feedback, human parameters of the SIM3 model for national and governmental CSIRTs are influenced by lack of resources, skills and experience.

The most challenging parameters concern training and mentoring of existing and new staff. All four certified national and governmental CSIRTs reported having this practice documented. Since new members of the team are tutored irregularly and in many cases by different team members, the process tends to be "re-invented" every time. The recommendation is to think about this process and to document it according to the team's needs.

Another challenge for national and governmental CSIRTs is to justify a sufficient external training budget. Reducing the availability of financial resources influences the ability of CSIRTs to train and certify staff skills, and recertification, in particular, might be put in doubt. Some teams argue that a wide range of video and online training is available, but lack of human networking means that teams do not have an opportunity to get to know one another to build up trust.

[43] https://www.enisa.europa.eu/activities/cert/events/10th-cert-enisa-workshop
[44] http://www.cert.org/
[45] http://www.egc-group.org/

6. Maturity of Technical Parameters

6.1 T-1.IT Resources List

6.1.1 Requirements

MINMUM LEVEL	DESCRIPTION
1	Implicit – awareness, knowledge in head, experience

The constituency of national and governmental CSIRTs is generally diverse and so is the range of resources (software and hardware) a CSIRT has to support. However, in order to achieve certification, a CSIRT should be able to know at least what kind of service, and, in particular, what kind of help and information the constituency is expecting.

In the case of a governmental CSIRT, it might be possible to gather more information on certain institutions (for example, on critical infrastructure providers or governmental institutions). This can be achieved by surveying constituents over time to obtain information on their IT resources. The results of this assessment should be kept in some organised form (for example, a configuration management database (CMDB) or other type of asset management).

For national CSIRTs it is more difficult, and in many cases not feasible, to maintain a complete list of resources of constituents, in which case information and advisories should be distributed in case of any major vulnerability. National and governmental CSIRTs should be trained and educated to handle any requirements of the constituency.

6.1.2 CERT.LV experience

CERT.LV's constituency is the whole country so the creation of a list of resources used by the constituency is neither practical nor achievable. There are some institutions with the highest priority, and for those certain information has been gathered, mostly concerning online resources and used content management systems (CMS). This information is kept in the user database where it is possible to filter, for example, all high priority institutions using certain CMS.

6.1.3 Comments from certified teams

Most CSIRTs maintain lists with information about constituencies' IT resources that sometimes are incomplete. Usually, more information is available about governmental institutions and critical infrastructure providers. Some teams mentioned that maintaining such a list is a challenging task and this information has to be properly protected since it can be sensitive. National CSIRTs have usually only a rough idea constituency's resources (for example, from information collected by public awareness campaigns, surveys etc), but mostly CSIRTs rely on their experience and ability to handle issues with all types of hardware and software.

6.2 T-2.Information Sources List

6.2.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

National and governmental CSIRTs should have at least one written procedure on how they obtain vulnerability and threat information, including a list of information sources. There might be additional information on each source (e.g. trustfulness, usability etc). A wide range of information sources is available for direct integration into CSIRTs' incident tracking systems and to be used for educational activities.

6.2.2 CERT.LV experience

CERT.LV has an information sources list that is integrated into the customer management system. Feeds from these sources are processed automatically and distributed to the constituents on a daily basis, and feeds on newest vulnerabilities and viruses are published daily on the CERT.LV web page. Several sources are used to prepare educational materials.

6.2.3 Comments from certified teams

All certified national and governmental CSIRTs mentioned that they maintain such a list in various forms – internal wiki or special systems (TARANIS, OTRS etc). The information sources list usually contains both media monitoring and public information sources, as well as more confidential sources of information.

6.3 T-3.Consolidated E-mail System

6.3.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

All CSIRT e-mail should be kept in one repository available for all CSIRT members on a need-to-know basis. Preferably, there should be a ticketing system or similar in place for managing e-mail which should be documented and accepted by the CSIRT management as a formal document.

6.3.2 CERT.LV experience

All e-mail sent to the central e-mail addresses of CERT.LV is kept in the ticketing system (in this case RTIR); the responses are also sent from that system and copies are kept there. All CERT.LV employees have access to this system. There are other e-mail lists used for particular purposes (e.g. for receiving contact information, for applying to events) which are available to all employees involved in the particular process, but no central archive is kept. The process is described in the handbook.

6.3.3 Comments from certified teams

All teams noted that they are using RTIR, which provides a consolidated e-mail system and allows some degree of automatization of processing incoming incident reports (for some teams up to 80% of incidents are handled automatically).

6.4 T-4.Incident Tracking System

6.4.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

There should be a formal document that describes how incidents are handled using a tracking system tool. A variety of these tools are available (e.g. RTIR, AIRT). Initial training on system usage for new employees should be available. Although Request Tracker systems are tailored for CSIRTs, every CSIRT has different needs and usually additional tailoring will be required, so it is recommended to have an in-house developer. Requirements and suggestions of those employees working daily with the tracking system should be taken into account as much as possible.

6.4.2 CERT.LV experience

CERT.LV uses the RTIR system (Request Tracker for Incident Response[46]). There are separate documents on the proper RTIR usage and incident life-cycle. The RTIR usage document explains the workflow of when to create an incident, when an incident report, etc. CERT.LV has an in-house developer to make minor adjustments to the system when needed.

6.4.3 Comments from certified teams

All teams mentioned that they are using RTIR for incident tracking. Teams noted that RTIR needs a good deal of work and adjustments but nothing better is available.

6.5 T-5.Resilient Phone

6.5.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

CSIRTS should be aware of their requirements for phone service. Although certification does not require a formal document, it should be included in the service provider's contract definitions of basic service with defined maximum outage time and/or time to resume service. Reasonable back-up or fall-back options are obviously mobile phones. National and governmental CSIRTs should also consider operation in a major crisis situation, possibly as part of a country's overall crisis management mechanism.

6.5.2 CERT.LV experience

CERT.LV is using landlines as a basic phone service, with requirements set out in the contract with the service provider. As a standard fall-back mechanism, mobile phones are available to all employees, with encryption features if needed. Other fall-back mechanisms include Skype[47] and Jabber[48] communications.

6.5.3 Comments from certified teams

Certified national and governmental CSIRTs use the host organisation's phone infrastructure and some of them have access to the national emergency network. In most cases, service level agreements are in place.

[46] https://www.bestpractical.com/rtir/index.html
[47] http://www.skype.com/
[48] http://www.jabber.org/

6.6 T-6.Resilient E-mail

6.6.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

Best practice is that CSIRTs maintain their own e-mail services. Encrypted connections for both incoming and outgoing e-mail are mandatory, and masking of the sender's IP address is a feature to consider.

In case the e-mail services are outsourced, a service level agreement should be in place with at least defined maximum outage time and/or time to resume services. Confidentiality issues should be seriously considered.

6.6.2 CERT.LV experience

CERT.LV e-mail services are provided by the host organisation and maintained by the members of the CERT.LV team. A wide range of security features are implemented.

6.6.3 Comments from certified teams

All certified national and governmental CSIRTs maintain their own e-mail services, though some make use of the host organisation's e-mail infrastructure too.

6.7 T-7.Resilient Internet Access

6.7.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

CSIRTS should be aware of their requirements for internet access. National and governmental CSIRTs should have more than one internet service provider or at least redundant physical connections. Service level agreements should be in place, defining at least maximum outage time and/or time to resume services.

If possible, governmental CSIRTs should be part of a governmental network for national crisis.

6.7.2 CERT.LV experience

CERT.LV has redundant connections from several ISPs, for both Latvian and foreign traffic. Redundant physical connections are in place. In addition, CERT.LV has an access point to the national crisis network.

6.7.3 Comments from certified teams

All teams use the host organisation's internet infrastructure; some teams mentioned a specific service level agreement with ISPs. All teams have connectivity from several ISPs, and some teams have access to the national emergency network.

6.8 T-8.Incident Prevention Toolset

6.8.1 Requirements

MINMUM LEVEL	DESCRIPTION
1	Implicit – awareness, knowledge in head, experience

National CSIRTs, in most cases, have a coordinating role, so this parameter can be omitted from the scoring. In case the CSIRT's role is not purely coordinating, the certification requirement is to be aware of the available tools for incident prevention.

Governmental CSIRTs may have the potential to cooperate more closely with the constituency, including options to recommend certain usage of tools and also to receive information collected from such tools, i.e. incident prevention systems, spam filters, virus scanning, etc.

Best practice for national and governmental CSIRTs which do not have direct access to the constituencies' infrastructure is to use honeypots and spam traps in order to detect activities in the network.

6.8.2 CERT.LV experience

CERT.LV as a national CSIRT has a mostly coordinating function. However, as a governmental CSIRT it has some activities in the incident prevention area, including spam traps, honeypots and direct information from some institutions. The CERT.LV mandate allows penetration testing and security audits for some groups of constituents which contribute greatly to the security infrastructure of these constituents.

6.8.3 Comments from certified teams

One national CSIRT has scored -1 in this parameter, i.e. it is not measured, while others have a toolset description in the handbook or internal wiki. Some teams provide self-service tools for the constituents, e.g. port scanning service. Some of the incident prevention information is published on the website. During certification, it is essential to prove that people can actually use the described toolset accordingly.

6.9 T-9.Incident Detection Toolset

6.9.1 Requirements

MINMUM LEVEL	DESCRIPTION
1	Implicit – awareness, knowledge in head, experience

It is important, especially for governmental CSIRTs, to obtain information about incidents when they happen or are about to happen. Most valuable would be direct data from the constituents (e.g. incident detection system (IDS) data, netflow data). Arrangements for getting such information should be possible for the governmental CSIRTs. Another option for CSIRTs, if legislation permits such an option, is to create a dedicated network of sensors for incident detection in the constituency.

It is possible for all national and governmental CSIRTs to gain information from external sources (such as Spamhaus, Team Cymru, Shadowserver, etc) about detected incidents in their constituency. If processed

accordingly, this information can provide targeted advice (for example, to ISPs and end-users) about incidents.

6.9.2 CERT.LV experience

CERT.LV uses external sources for obtaining information and providing targeted warnings to constituents about incidents. Legally, CERT.LV has a right to collect data flows from the constituents on the basis of mutual agreement. This possibility is used to deploy early warning system sensors in the constituency to receive very valuable information for incident detection.

6.9.3 Comments from certified teams

One team has pointed out that they do not do much for incident detection, so a -1 scoring could be considered, although another mark was given during the certification process. Other teams have tools that are well documented in the wiki or internal documents. During the certification, a demonstration of tools was carried out by some teams.

6.10 T-10.Incident Resolution Toolset

6.10.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

Certification requirements ask at least for an internal description of available tools for incident resolution. The range of tools can be wide, from pure basics (Whois, Traceroute) to advanced laboratories and toolsets. National and governmental CSIRTs should be able to deal with almost any kind of incident, so they should possess a corresponding set of tools – forensics, reverse engineering and web application analysis toolkits should be available at least.

The CSIRT community is open in sharing information and uses different types of tools. For most needs, free open source tools are available that allow CSIRTs to manage their functions without additional expenses. For commercial tools, there can be a discount option, especially for national and governmental CSIRTs.

6.10.2 CERT.LV experience

Over many years of operation, CERT.LV has gained experience in using a wide range of tools for incident resolution. Most of them are open source but some are developed in-house. Coming from an academic background, CERT.LV has strong links to the scientific community that allow the development and usage of some experimental tools.

6.10.3 Comments from certified teams

All certified national and governmental CSIRTs have incident resolution tools which are well documented. One of the teams has a public presentation about tools used for incident resolution.

6.11 General comments on technical parameters

According to the Trusted Introducer experts' opinion, only new teams have problems with using tools. Experienced teams have all the tooling in place.

If the team has a good balance of technical and process oriented people, this ensures sufficient technical capabilities which are properly documented.

7. Maturity of Process Parameters

7.1 P-1.Escalation to Governance Level

7.1.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

The escalation process to the upper management of national and governmental CSIRTs and to governance level of constituents needs to be formalised and approved by at least the management of a CSIRT. The formalised process needs to take into account different scenarios, while the escalation process needs to incorporate the severity of an incident and emergency situations. If a national and governmental CSIRT acts as a coordination entity, there should be a mechanism that sets deadlines for a responsible person to handle an incident and provide feedback to the CSIRT. If these deadlines are not met, there should be the ability to contact the upper management of the organisation.

Management of national and governmental CSIRTs should have a clear understanding of how to reach the upper levels of government in appropriate cases.

7.1.2 CERT.LV experience

CERT.LV acts under the direct supervision of the Ministry of Defence, which is the responsible institution for IT security in Latvia. Besides the IT Security law, there is the delegation agreement between CERT.LV and the Ministry of Defence that is concluded yearly and defines, among other things, the information flow between the institutions.

According to the law, if CERT.LV detects a security incident that jeopardises national security, it shall inform the Minister for Transport, the Minister for Defence, the Minister responsible for the sector in which the incident occurred and the competent State security institution. If a breach of security or integrity has been detected that has had a significant impact on the operations of electronic communications networks or the provision of services, CERT.LV should notify the State administrative institutions of the European Union Member States and ENISA regarding what has happened.

As a final escalation point – in the case of a severe crisis that endangers the State, the Cabinet of Ministers may take a decision to transfer the tasks, rights and resources of CERT.LV to the National Armed Forces.

When coordinating the usual security incidents, the incident handling process of CERT.LV sets the deadline for contacting the governance level of the constituent.

7.1.3 Comments from certified teams

Escalation to the governance level for certified teams is very well established. It should be documented in the internal procedures with the host organisation or formalised in the agreement with the government, or documented in the handbook or wiki. It is also important to test the escalation in some exercises.

7.2 P-2.Press Escalation

7.2.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

The press escalation process should describe how a national and governmental CSIRT reaches the host organisation's press office. There should be clear boundaries about what a national and governmental CSIRT can disclose to the public without coordination with the host organisation, and what messages should be reconciled. An example of messages that need coordination at governmental level could be large-scale attacks on governmental institutions or critical infrastructure. Up-to-date contact information and time restrictions are important in such cases.

7.2.2 CERT.LV experience

As stated before, the flow of information between CERT.LV and the Ministry of Defence is described in the delegation agreement. The law gives CERT.LV the mandate to inform the public or require the relevant electronic communications merchants to do so, where it determines that disclosure of a security incident is in the public interest.

In cases of specific incidents, the message is also coordinated with the affected institution.

A lesson learned from the crisis exercises is that in the case of crisis, the message to media is coordinated with the State Chancellery which is the central public administration service. No particular agreements with the press or media are in place, but contact details are available for major radio stations, TV channels and portals.

7.2.3 Comments from certified teams

Press escalation is well documented for the certified teams. In most cases, it is documented in the procedures with the host organisation as well as in the handbook or wiki. Host organisations tend to have various sized communication departments, which can be involved if a CSIRT has a large incident to deal with.

7.3 P-3.Legal Escalation

7.3.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Legal escalation might take place in different cases – coordination and legal support in a crisis situation and incident handling (including international incidents), and administrative tasks such as approving agreements and *Memoranda* of Understanding. The legal process can be exercised as part of CSIRT exercises, especially

international exercises. As in all escalation processes, there needs to be up-to-date contact information for the legal counterparts.

7.3.2 CERT.LV experience

The CERT.LV process of legal escalation is set out in the delegation agreement with the Ministry of Defence. One of the requirements of the agreement is to submit for approval international agreements and Memorandums of Understanding.

CERT.LV involves its legal expert in various available international exercises when possible.

7.3.3 Comments from certified teams

Legal escalation for the certified national and governmental teams is established in the procedures with the host organisation and detailed in the handbook or wiki.

7.4 P-4.Incident Prevention Process

7.4.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

National CSIRTs can mainly prevent incidents by raising awareness, educating constituents and issuing advisories. For governmental CSIRTs, influence can be more direct depending on cooperation between the institutions. Procedure for usage of the tools mentioned in parameter T-8 should be written down, made available on a need-to-know basis and regularly updated (a solution such as wiki could be appropriate).

7.4.2 CERT.LV experience

CERT.LV works on incident prevention mainly by awareness-raising activities, and issuing advisories and targeted warnings to constituents. As mentioned in chapter 6.8.2, CERT.LV also has more direct incident prevention initiatives for certain groups of constituents.

The process of incident prevention is written down and available to employees in the handbook and the internal wiki.

7.4.3 Comments from certified teams

The incident prevention process for all certified national and governmental CSIRTs is documented in line with the corresponding toolset (parameter T-8). A high-level description is usually available in the handbook and more details are available in the internal wiki.

7.5 P-5.Incident Detection Process

7.5.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

The procedure for usage of the tools mentioned in chapter 6.9 should be written down, made available on a need-to-know basis and regularly updated (a solution such as wiki could be appropriate). When obtaining direct information from constituents, there might be a need for special arrangements regarding confidentiality of data.

7.5.2 CERT.LV experience

CERT.LV uses an early warning system deployed in constituents' networks as well as automated processing of outside sources. The process of using incident detection tools is written down and available to the employees in the handbook and the internal wiki.

7.5.3 Comments from certified teams

The incident detection process is documented in line with the incident detection toolset (parameter T-9), and in most cases the handbook and wiki are also used.

7.6 P-6.Incident Resolution Process

7.6.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

The procedure for usage of the tools mentioned in chapter 6.10 should be documented, made available on a need-to-know basis and regularly updated (a solution such as wiki could be appropriate).

7.6.2 CERT.LV experience

CERT.LV has an incident resolution workflow that is documented and available to employees. The procedure defines any incidents' life-cycle.

7.6.3 Comments from certified teams

The incident resolution process is documented in line with the incident resolution toolset (parameter T-10), and in most cases the handbook and wiki are used. One team has published its incident handling process online on the web page describing how the team can participate in the incident resolution. In one case, these documents have internal security classification.

7.7 P-7.Specific Incident Processes

7.7.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

CSIRTs need to understand whether different workflows are required for different types of incident. Procedures and workflows should be developed accordingly (either as one general workflow that fits all incidents or several different workflows for different types of incident).

7.7.2 CERT.LV experience

CERT.LV has no specific workflow for different kinds of incident. The CERT.LV incident resolution process is designed to fit all incident categories, taking into account priority of the incident.

7.7.3 Comments from certified teams

Three certified national and governmental CSIRTs have separate processes for different kinds of incident. These processes are documented in the internal wiki, and are used and updated frequently. Examples of incident types that have different workflows are DDoS incidents, PKI-related incidents, phishing, malicious IP addresses and URLs, and Advanced persistent threat process. Different processes also require different toolsets.

One team, however, has one workflow, which works for all types of incidents.

7.8 P-8.Audit/Feedback Processes

7.8.1 Requirements

MINMUM LEVEL	DESCRIPTION
4	Explicit, audited on authority of governance levels above CSIRT head – subject to outside control/audit

This is one of strictest requirements of certification where level 4 scoring is required, and an explicit and active audit process from levels above the national and government CSIRT head should be in place. An audit should include feedback from management or customers and a follow-up process in order to ensure improvement and accountability. As part of the process, regular reports to the governing or supervising institution should be prepared. Some kind of reporting to the public should be considered in the case of a national and governmental CSIRT.

7.8.2 CERT.LV experience

CERT.LV has strict requirements and deadlines for quarterly reports for both tasks and finances. Reports are reviewed and accepted in writing by the Ministry of Defence within the set timeline. Non-compliance with requirements from the Ministry of Defence may result in termination of the delegation contract.

7.8.3 Comments from certified teams

Certified teams have differing approaches to the audit parameter. In some cases, regular security tests for the CSIRT systems are performed by external auditors. In two cases, annual review with the corresponding ministry or customers takes place, while for some teams, a process for external audit and assessment is in place.

7.9 P-9.Emergency Reachability Process

7.9.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

A certification requirement asks for a formal document that describes the reachability of a CSIRT in cases of emergency outside the normal office hours. For national and governmental CSIRTs, emergency reachability 24/7 as an international contact point should be considered[49]. At an international level, organisations such as Trusted Introducer and FIRST can help with sharing contact information between CSIRTs (both have contact information directories that are available only to accredited and certified teams/full members). National and governmental CSIRTS of the EU should be part of the planned cooperation network where ENISA is envisaged to provide its support and where it can act as the independent body for maintaining the respective information.

7.9.2 CERT.LV experience

CERT.LV outsources its 24/7 helpdesk function to the host organisation. Helpdesk operators are instructed on how to reach the responsible CERT.LV employee outside normal office hours using mobile phone numbers. Mobile phone numbers of the CERT manager and the deputy manager are available to the upper level management of the Ministry of Defence, police, security services and members of the Security Council. International emergency contacts are available and up to date in the Trusted Introducer contact database. Alternatively, communication options such as Skype and Jabber are available.

7.9.3 Comments from certified teams

Emergency reachability is very well ensured by all certified national and governmental CSIRTs. Methods used 24/7 as well as other contact details are available online on the website, in the agreements with customers, on the Trusted Introducer and FIRST databases, and in the RFC2350 document.

7.10 P-10.Best practice e-mail and web presence

7.10.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

National and governmental CSIRTs should handle generic security-related mailbox aliases such as security@, abuse@. However, not all e-mail aliases suggested in the SIM3 model are relevant for national and

[49] https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012 chapter 7.1 Human resources

governmental CSIRTs. For example, hostmaster@, webmaster@ and postmaster@ are more relevant to those CSIRTs serving a particular organisation.

Also, web presence for national and governmental CSIRTs is a must, and there has to be an English part of the website available. The web page should clearly describe at least the constituency, services and contact information of the CSIRT. Teams might consider publishing the contact information of all employees or just the 'public facing' part.

7.10.2 CERT.LV experience

Usual contact information for CERT.LV is available in the RFC2350 document and on the website[50] of CERT.LV, including the e-mail addresses (name.surname@cert.lv) and public PGP keys of all employees. The usual e-mail address for reporting incidents is cert@cert.lv. CERT.LV also supports a wide range of aliases such as abuse@cert.lv, spam@cert.lv, etc. Not all aliases specified in the SIM3 model exist naturally for CERT.LV. It remains to be seen if they are set up for certification.
Other dedicated e-mail addresses are available for registration to events, to update contact information, etc.
CERT.LV has a regular website containing information on news, events, legislation, examples, etc. CERT.LV maintains an information security awareness-raising site: www.esidross.lv, which provides information on whether the IP address of the visitor is infected according to the CERT.LV data.

7.10.3 Comments from certified teams

This requirement is tested during certification. Testing is difficult if the team's domain is not entirely clear. Certified national and governmental CSIRTs have different experiences – some teams set up missing aliases during the certification process, but others have argued that missing aliases are not needed. If a CSIRT is maintaining its own e-mail system then setting up extra aliases is very easy. If the host organisation is large enough, it might be that not all test messages for this parameter reach the CSIRT.

7.11 P-11.Secure Information Handling Process

7.11.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

National and governmental CSIRTs handle sensitive information on a day-to-day basis. There must be a procedure for handling and sharing information of different confidentiality levels. If there is national legislation in place for sensitive information handling, it must be included in the procedure.

Information classification should be in place and applied for all kinds of information.

[50] https://cert.lv/section/show/14

The international de facto standard for CSIRT cooperation is ISTLP (Information sharing traffic light protocol[51]). Its use ensures successful international cooperation, and it is also practical and simple to implement.

In addition, technical means of protecting information should be in place and observed, such as sending and receiving secure e-mail with PGP support, secure voice communication solutions, storing and back-ups (including off-site back-ups), and secure destruction of disks and other media.

All employees should be instructed on how to handle sensitive information.

7.11.2 CERT.LV experience

CERT.LV has regulations on handling sensitive information in accordance with national laws. All employees are required by law to have security clearance, which means they have passed background checks by security authorities, and also are required to participate in training for secure information handling.

CERT.LV also has a separate technical solution for sensitive information exchange with governmental institutions.

Information on how to contact CERT.LV securely using PGP is published on the website[52].

Traffic light protocol is used for both national and international communication.

7.11.3 Comments from certified teams

A secure information handling process is part of the security policy for most teams. Separate processes for usage of PGP and TLP in most cases are in place and documented in the handbook or wiki. In one case, different communication media are used for different parts of the constituency. Some information on secure incident handling is also provided in the Trusted Introducer database for the teams.

National and, particularly, governmental CSIRTs must also handle sensitive information classified according to national legislation or NATO and EU legislation. Special procedures for that are defined by law.

7.12 P-12.Information Sources Process

7.12.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

The procedure for usage of the information sources mentioned in chapter 6.2 should be written down, available on a need-to-know basis and regularly updated (a solution such as wiki could be appropriate).

[51] https://www.trusted-introducer.org/ISTLPv11.pdf
[52] https://cert.lv/section/show/14

7.12.2 CERT.LV experience

The CERT.LV Handbook contains an internal procedure on how information sources are handled and used. CERT.LV's internal wiki contains an up-to-date list of information sources.

7.12.3 Comments from certified teams

All certified national and governmental CSIRTs have processes in place on how to handle information sources described for parameter T-2. The most sophisticated system currently in use is TARANIS[53].

7.13 P-13.Outreach Process

7.13.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

This parameter is about reaching out to the constituency of a CSIRT outside the regular incident handling process. This includes public and media releases, and different awareness-raising activities. Maturity requirement is to have a formal document within the CSIRT. It is important for a national and governmental CSIRT to communicate information about IT security as well as about the CSIRT as an entity. This contributes to the CSIRT incident solution capabilities in two ways: user awareness-raising decreases the risk of incidents and trust and visibility of the CSIRT are increased.

Outreach activities can take different forms, for example:

- events (seminars, workshops) targeting particular groups (from schoolchildren to IT professionals and managers);
- different types of educational materials;
- participation in partners' organised events nationally and internationally;
- support to the dedicated groups of experts and discussion forums;
- participation in TV news editions, radio shows, etc;
- regular contributions to press, media and news agencies.

CSIRT employees should be aware of the outreach process and contribute to it as much as possible.

7.13.2 CERT.LV experience

CERT.LV as a national and governmental CSIRT has a variety of partners and corresponding outreach activities, described in the table below. CERT.LV is trying to connect these activities with outside initiatives, for example, taking part in the European Cyber Security Month[54] that is supported by ENISA.

PARTNER	OUTREACH ACTIVITIES
State and local governmental institutions	Dedicated warnings and advisories

[53] https://www.ncsc.nl/english/Incident+Response/monitoring/taranis.html
[54] https://cybersecuritymonth.eu/

	Technical training Workshops/seminars Awareness-raising campaigns for employees
Internet service providers	'Responsible internet service provider' initiative Warnings and advisories Participation in events
Critical infrastructure providers	Dedicated warnings and advisories Technical training Workshops/seminars Security audits Penetration tests
Internet users	Workshops/seminars Educational activities Computer check-up (twice a year) European Cyber Security Months organised by ENISA (various events in October every year) Outreach portal[55]
Security professionals	Group of information security experts[56] Participation in technical exercises

CERT.LV has a social presence on Twitter, Facebook and in the Latvian social network: draugiem.lv.

7.13.3 Comments from certified teams

For most teams this process is well established and set out in the handbook or wiki. The host organisation's partnership department is involved in the process in one case. One certified team has also developed a social media usage policy to ensure consistency, while another team suggested using exercises to discover which parts of the constituency are not yet reached out to properly.

7.14 P-14.Reporting Process

7.14.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

[55]https:// www.esidross.lv/
[56] https://cert.lv/section/show/17

As part of consistent operation, national and governmental CSIRTs should be accountable for their activities, not only to the supervising organisation but also to the general public. The reporting process has to be properly documented in the internal documents or wiki.

CSIRT employees should be aware of the reporting process and contribute to it accordingly.

7.14.2 CERT.LV experience

CERT.LV produces quarterly reports for the Ministry of Defence (see information for the parameter P-8). Based on those reports, CERT.LV produces quarterly public reports which are available online[57]. In addition, annual reports are produced for both the supervising institution and general public but the level of detail and classification differs between the two versions.

7.14.3 Comments from certified teams

Reporting to the management is well documented for all certified national and governmental CSIRTs as well as supported by tools. Mechanisms used differ however – some teams have annual or quarterly reports, others provide management with financial reporting while other reports target a wider audience.

7.15 P-15.Statistics Process

7.15.1 Requirements

MINMUM LEVEL	DESCRIPTION
3	Explicit, formalized on authority of CSIRT head – formal document accepted by CSIRT management

Taking into account incident classification, there should be a formal document describing how statistics on handled incidents are created and disclosed. The statistics process might be part of the whole reporting process.

7.15.2 CERT.LV experience

CERT.LV gathers incident statistics each month. Incidents are divided into high and low priority (see chapter 4.7 about incident classification). Statistics are made available on the CERT.LV web page and in the quarterly and annual reports.

7.15.3 Comments from certified teams

If a team reports only to management and does not publish any statistics for the constituency, then it can score -1 in this parameter (one of the certified teams was scored like this). Other teams publish either annual or more frequent statistics online. However, teams have noted that usage of common metrics which could be compared with other teams would be more useful (FIRST metrics working group is pursuing this area[58]).

[57] https://cert.lv/section/show/48
[58] https://www.first.org/global/sigs/metrics

7.16 P-16.Meeting Process

7.16.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

Internal meetings should be held at least once a month in order to keep everybody up to date about everyday activities. These should not be very formal meetings but some kind of minutes should be kept as a point of reference. Also, regular meetings in smaller groups within the CSIRT on dedicated questions should be encouraged. Operational meetings and shift handover meetings should be considered for better information exchange on operational issues.

7.16.2 CERT.LV experience

CERT.LV has monthly meetings of all team members. During the meeting each team member talks about main activities and plans for the next month and the event calendar is updated. Formal notes are kept, with rotation of the responsible note-taker.

CERT.LV technical division has dedicated meetings in order to encourage technical discussion. Information exchange between employees is kept informal however, considering the 'need to know' principle.

The meeting process is documented in the handbook.

7.16.3 Comments from certified teams

All teams have regular meetings in place and the meeting process is documented in either the handbook or wiki. In only one case has a more formal document been mentioned. The frequency of the meetings varies: operational meetings are usually more often (even daily for the duty officer hand-over) while organisational meetings are less often (weekly or bi-weekly).

7.17 P-17.Peer-to-Peer Process

7.17.1 Requirements

MINMUM LEVEL	DESCRIPTION
2	Explicit, internal – internal informal document/procedure written down

The importance of the peer-to-peer process should be understood. Actionable information exchange can help CSIRTs in everyday activities, and the support of an international organisation is essential.

7.17.2 CERT.LV experience

The peer-to-peer process is not formalised in CERT.LV, though broad cooperation with other CSIRTs takes place. Steps towards formal cooperation within three Baltic States are being taken and technical cooperation is already on-going. Memorandums of Understanding have been concluded with several countries' CSIRTs. CERT.LV participates in joint exercises with the Baltic countries' CSIRTS as well as other European CSIRTs.

7.17.3 Comments from certified teams

The peer-to-peer process is well understood and documented for certified national and governmental CSIRTs. It is documented in the handbook or wiki, including information on EU-SOPs[59]. Most of the teams include responsible persons for particular cooperation areas in the same wiki pages.

7.18 General comments on process parameters

Fulfilling the requirements of process parameters can be challenging for some teams. If a team consists more of operational/technically oriented people, then there could be a noticeable lack of procedures. If the team is more focused on procedures and politics, it might lack experience and tools.

An ideal certification process would be for a well-balanced team, for example, for an operational team with someone experienced enough to take care of the procedures. A mixture of capabilities results in a smoother certification experience.

[59] https://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa

8. Conclusions

In general, national and governmental CSIRTs must reach a higher maturity level and improve in order to cope with the evolving cyberspace and its threats and vulnerabilities. The SIM3 model can be used as a tool to assist in this process as well as to obtain an independent evaluation of CSIRT capabilities.

In order to evolve their capabilities, teams must take a step back and objectively assess their state of internal and external processes and procedures. Questions which have to be answered include: is the team consistent, and are their capabilities sufficient to fulfil its functions? Existing CSIRT certification is a suitable tool for this purpose because it evaluates whether the team is compliant with its mission statement rather than some general compliance criteria.

It is important for teams to understand that this is not just an audit to check and validate their current status – it is a process to evaluate a team's current standing and identify areas where improvement is most needed. Even when going through the recertification process, the team has to show its advancement in maturity during the past three years.

It is important for every team to do its homework before applying for the certification process – mainly through self-assessment – but usually many of the required parameters are already or can easily be fulfilled. The team has to be prepared to "tell the truth" and be honest with themselves and the evaluating experts; only this approach can be beneficial for the team.

The evaluating experts usually try to see if a team's processes are too complicated, and might suggest some improvements. The certification workshop allows time to talk about processes and rethink them. It is useful for the team to look at itself from a different angle.

Based on the input from already certified national and governmental CSIRTs, several practical recommendations are summarised below.

Practical recommendations (DOs):

- Management support: Involve senior management in the certification process from the beginning to ensure sufficient resources and approvals.
- Resources: Make sure there are sufficient resources available for the certification – both manpower and finances.
- Person in charge: A dedicated person to handle the certification process will make it more productive and will ensure smoother and faster results.
- Handbook: Have a good handbook document approved by the management (resulting in a level 3 document).
- Procedures: Develop procedures consistent with the team's mission statement and everyday activities. Keep procedures up to date.
- RFC2350: Have a good RFC2350 document in place and keep it updated.
- Website: Have the public website and the main reference documents and contact details (i.e. RFC2350) also in English.
- Documentation: Have all existing documents for the certification in one place, in one folder – it will smooth the certification process and can be used by the team itself.
- Internal wiki: Have an internal wiki instead of lengthy documents; wiki is easier to use and to update in case of changes.

- Rotation: Assign a new team member every year to the certification and document update process, the team member will gain an excellent understanding of how the organisation works.
- Education and training: Have the process for training new employees documented, to avoid 'reinventing the wheel' every time.
- External networking: Participation of national and governmental CSIRTs in CSIRT networks, such as TF-CSIRT, FIRST and ENISA's annual workshop, is essential to understand the environment and be a successful and productive part of it.
- Self-assessment: Carry out a self-assessment of the team's capabilities before applying for certification. ENISA can assist the Member State based on its 'Article 14 request' procedure[60].
- Constant improvement: After the certification do not stop, but consider how to improve more. Devise a strategy on how to reach the next level, paying special attention to the parameters where the team scored lower.

Practical recommendations (DON'Ts):

- Do not use certification as a goal itself, rather consider improvements that could be made and TI certification as an added bonus;
- Do not be dishonest during the process of self-assessment and in the process of certification otherwise it would not be possible to reach higher maturity;
- Do not be intimidated by the process – it might look more difficult than it is in reality;
- Do not start the certification process without exploring the available information and resources; consult other teams, TI experts and ENISA.

Some teams think that the ultimate goal would be to advance all parameters to level 4 of the SIM3 model. Usually, that is not needed because in many cases it would be a waste of resources to audit all aspects of a team's work. When documents are approved by the team leader (level 3 of the SIM3 model), they might become more valuable and useful, because it is something all the team considers and agrees upon. For many parameters, level 4 is not needed or even feasible.

A team might have changed its structure in the timeframe between certification and recertification so it is important during recertification to confirm that all processes work within the new structure.

CSIRT maturity is a process that needs time for the team to improve in every aspect of its work. The TI certification scheme is a tool that allows the team to check its performance against its own mandate and to shed light on the existing gaps. Certification is more about understanding the process and finding the cause of problems than about achieving the right marks.

This document should server as a guidance tool for all, but especially national and governmental CSIRTs that are aiming to advance their maturity in all aspects related to CSIRT work. Honest feedback about the certification process and parameters' implementation from already certified teams, as well as from a team in the process of getting ready for certification, is a practical help for all teams considering advancement and certification.

[60] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-02-15-992-EN-N

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

ISBN: 978-92-9204-164-9
DOI: 10.2824/214073