ENISA CSIRT maturity assessment model

FINAL

VERSION 2.0

EXTERNAL

30 APRIL 2019

www.enisa.europa.eu
European Union Agency For Network And Information Security

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.

Editors

ENISA

Contact

For contacting the authors please use cert-relations@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The authors would like to thank the members of the European Union CSIRTs for their help during the review phase and acknowledge the validation of the report during the 3rd informal CSIRT network meeting that was held in The Hague, The Netherlands on 9th November 2016.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-292-9, DOI 10.2824/860039

Table of Contents

Executive Summary

The NIS Directive [6] aims at creating a CSIRT Network “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation”. The Directive states that each Member State shall designate one or more CSIRTs that shall comply with a set of defined high-level requirements. In order to provide input to the designated CSIRTs on this topic, ENISA contracted a study on the maturity aspects for this type of CSIRTs, narrowed down to the national teams expected to join the CSIRT network – the results of which are presented here.

The study takes all relevant information sources into account, with a special emphasis on the NIS Directive, the various ENISA reports on CSIRT capabilities, maturity and metrics, and on the SIM3 maturity model for CSIRTs which is a best practice document widely used in Europe, but also outside.

The first lesson learnt is that a sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NIS Directive requirements.

The second lesson learnt is that the three-tier approach towards maturity levels that ENISA adopted in the 2013 report ‘CERT community - Recognition mechanisms and schemes’ can be used to define three levels when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and advanced.

The report specifies a proposed definition of those three levels for the benefit of the CSIRT Network created by the NIS Directive, coupled with a validation process based on self-assessments and peer-assessments. No actual certification is prescribed, however the highest level advanced has been defined at the level of the existing CSIRT Certification scheme in Europe, which means that certification is within reach once that maturity level has been reached.

By adopting the proposed approach, the CSIRT Network will have immediate access to a clearly laid out CSIRT maturity improvement process, that is both implementable and sustainable. A growth path is suggested that reaches basic level within one year, intermediate two years later and advanced another two years later: a total of five years maximum. Basic level already allows a minimum of successful co-operation between teams on incident handling, the higher levels are needed to allow the members of the CSIRT network to interact on all levels, including pro-actively, thus truly giving meaning to the word CSIRT Network.

1. Introduction

The EU Network and Information Security Directive (NIS Directive) aims to create a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". [1] The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in the Directive's point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process. The Directive gives high-level requirements that designated CSIRTs must observe, and tasks that they must perform. In order to provide input to the designated CSIRTs on this topic, ENISA has contracted a study on CSIRTs capabilities and parameters that represent teams' maturity for this type of CSIRTs. For the purpose of this study the designated CSIRT was defined as the national CSIRT. The results of this study are presented here.

2. Methodology

The work in this project focused on the maturity aspects of the CSIRT portfolio. Initially, stock- taking of currently existing and used assessment parameters and recommendations or good practices to evaluate CSIRT maturity (capabilities) in Europe was performed – the CSIRT maturity model SIM3 (see 2.1) was a specially important source of such parameters. The result of that stock-taking was the identification of areas where assessment parameters are not yet optimally defined or tailored to the needs of national CSIRTs (according to the NISD and its obligations for dedicated CSIRTs). The outcome of the project elaborates on these areas and parameters that have to be considered when the national CSIRTs build their national CSIRT capabilities according to the NIS Directive obligations and/or when a national CSIRT wants to improve their maturity and prepare for the existing certification. The results presented will build upon the ENISA reports: *CSIRT Capabilities: how to assess maturity? Guidelines for national and governmental CSIRTs (2015)* – and – *CERT community - Recognition mechanisms and schemes* (2013).

2.1 Input sources

Input was considered from the following areas:

1. The above-mentioned ENISA reports *CSIRT Capabilities: how to assess maturity? Guidelines for national and governmental CSIRTs* [2] – and – *CERT community - Recognition mechanisms and schemes* [3]
2. SIM3 model for CSIRT self-assessment and certification (generic evaluation scheme for any type of CSIRT) [4]
3. Further ENISA baseline capabilities recommendations for national and governmental CSIRTs in Europe (specific recommendations for national and governmental type of CSIRT) [5]
4. NIS Directive – tasks and requirements of the dedicated (national) CSIRT (obligations for national (dedicated) CSIRT in the European Union [6]
5. GFCE CSIRT Maturity Kit [7]
6. Recommendations towards the use of SIM3 by members of the Nippon CSIRT Association [8]
7. FIRST Site Visit Requirements and Assessment [9]

2.2 Input evaluation

ENISA jointly worked with the contractor on assessing and structuring the input sources, especially the ENISA baseline capabilities documents and the NISD. After extensive mapping and visualisation of all aspects and parameters involved, it was concluded that mapping all of these onto the SIM3 architecture proved to be a highly workable approach. This allowed us to research all existing SIM3 parameters, and relate them with the NISD, ENISA documents and all other sources of input and come to recommendations as to how NISD and ENISA baseline capabilities can be translated into a sustainable system of measurable parameters, on which a progress in CSIRT maturity can be based.

3. Maturity Approaches

This chapter shortly re-iterates important approaches towards the topic of CSIRT maturity and concludes with a proposal how to combine these in one sustainable approach.

3.1 ENISA

3.1.1 CERT community - Recognition mechanisms and schemes

In ENISA's 2013 document *CERT community - Recognition mechanisms and schemes,* there is an analysis of various approaches worldwide in regard the topic of CSIRT maturity. One of the document's main features is the proposal of a three-tier CERT maturity model:

	Summary	**Characteristics**	**Organisation/mechanisms**
Tier 1	*Fundamental* (Essential, indispensable)	CERT is being established and trying to earn recognition in the CERT community (based on individual trust building).	ENISA: *A Step-by-Step Approach on How to Set up a CSIRT* (2006) ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009) ENISA: *Map of CERTs and Inventory of CERT Activities in Europe* (2005, constantly updated) TF-CSIRT/TI: 'Listed' status
Tier 2	*Baseline* (Steady, Sure-Footed)	CERT has baseline capabilities (operations) in place and its team representative gained trust among the CERT community.	ENISA: *Baseline Capabilities for National/ Governmental CERTs – Policy recommendations* (2010, 2012) IETF: *RFC-2350* (2003 update) TF-CSIRT/TI: 'Accreditation' FIRST: 'Full Membership' APCERT: 'Membership' CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)
Tier 3	*Advanced* (Stable, Well-Balanced)	CERT has a complete set of capabilities in place and has established a stable place in the community (no longer dependent on individuals from the team).	ENISA: *n/g CERT standard capabilities mechanism* (2014) ISO: *ISO 27035* (2011 update) TF-CSIRT/TI: 'Certification'

		These capabilities are all documented.	

This model is then further analysed on the basis of 8 assessment categories:

1. Type of approach (organisation)
2. Requirements for CERTs
3. Validation process
4. CERTs' focus: type and region
5. Benefits and added value of the mechanism
6. Definitions and terminology
7. Keeping the mechanism up to date
8. Promoting the mechanism and CERTs' training

And finally an important conclusion is reached, quoted here:

The number of mechanisms that exist for use by CERTs suggests that there may be room for harmonisation of certain aspects of these mechanisms. Targeted harmonisation could benefit both the organisations that offer mechanisms and CERTs that use them. For CERTs, harmonisation of these mechanisms can make it easier for them to associate with more CERT community organisations that offer these mechanisms. From the perspective of these CERT community organisations, harmonisation could enable cooperation with other similar organisations, and allow them to more easily make use of each other's existing resources. All of these potential advantages are about possible gained efficiencies, which is important given that these mechanisms should be about helping CERTs reach higher stages of maturity and better serve their constituents.

The 2013 document identifies several areas of possible harmonisation. Two of them stand out in the context of this report:

- Requirements for CERTs
- Validation process

3.1.2 CSIRT Capabilities: how to assess maturity? Guidelines for national and governmental CSIRTs

ENISA's 2015 document *CSIRT Capabilities: how to assess maturity? Guidelines for national and governmental CSIRTs* [2] aims to be a guiding tool for national and governmental CSIRTs which are considering to improve their maturity. It builds on the ENISA document discussed in 3.1.1. It starts with noting that in Europe the predominantly used maturity scheme is that of the Trusted Introducer, which essentially coincides with the three-tier model described in 3.1.1, and offers the levels:

1. Listing – the team is operational and contact information is available to other teams.
2. Accreditation – the team is fully functional, services are defined according to RFC2350, etc.
3. Certification – the team has reached an appropriate level of maturity.

The ENISA document then goes on to explain how the SIM3 CSIRT maturity model is the benchmark model for Certification – but is also a very suitable tool for self-assessments of CSIRTs with the aim of improving maturity.

The SIM3 model is explained. It consists of 44 parameters; quantities that are measured in regard maturity. Each parameter belongs to one of the following categories:

- O- Organisation
- H – Human
- T – Tools
- P - Processes

These categories have been chosen in such a way that the parameters in there are as mutually independent as possible. What SIM3 measures are the levels for each parameter. Simplicity has been reached by specifying a unique set of levels, valid for all of the parameters in all of the categories:

- 0 = not available / undefined / unaware
- 1 = implicit (known/considered but not written down, "between the ears")
- 2 = explicit, internal (written down but not formalised in any way)
- 3 = explicit, formalised on authority of CSIRT head ("rubberstamped" or published)
- 4 = explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis (subject to control process/review)

The ENISA document then goes on to detail all 44 parameters and comments on how they work in the everyday CSIRT practice in Europe – as various teams use SIM3 and several have been Certified based on the same model. An important conclusion reached is:

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.

3.2 EU NIS Directive

On 6 July 2016, the Directive on security of network and information systems (the NIS Directive, referred to here as NISD) was adopted by the European Parliament. Article 9 of NISD states:

Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

And NISD continues to state that:

- *The CSIRTS have adequate resources to effectively carry out their tasks*
- *Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs*
- *Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level*
- *Member States shall inform the Commission about the remit, as well as the main elements of the incident- handling process, of their CSIRTs*
- *Member States may request the assistance of ENISA in developing national CSIRTs*

Annex I of NISD is labelled *REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)* and is quoted here in full because of its great relevance for the national/governmental CSIRT community inside the EU:

(1) Requirements for CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.

(2) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network.

(b) CSIRTs shall establish cooperation relationships with the private sector.

(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes.

3.3 Assessing and improving CSIRT maturity based on measurable parameters

The project team evaluated in depth all input as referred to in section 2.1, and gave special significance to the ENISA documents discussed in section 3.1 and to the NISD discussed in section 3.2.

Based on that evaluation the following conclusions stand out:

1. A sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NISD requirements, and on recent insights as e.g. formulated by ENISA in their 2015 report on this topic[1].
2. A three-tier approach towards maturity levels is recognised both by ENISA and by *TF-CSIRT/Trusted Introducer*, the European cooperation body of all types of CSIRTs. It is possible to tie that in to the SIM3 maturity model by introducing, again, three levels of increasing maturity. For the sake of this report these levels have been labelled *basic*, *intermediate* and *advanced* – the latter, most mature, level connecting with the existing CSIRT Certification scheme in Europe. It is important to note that no exact 1:1 mapping between these three levels and the older schemes is proposed here – but rather a unified, sustainable approach meant to serve especially the "CSIRT Network" required by the NISD.

The next chapter details this proposed approach.

[1] SIM3 in its current version was essentially written in 2009 – since then there were only minor updates. A revision of SIM3 towards "version 2" is currently being undertaken, the results of which are expected in 2017. Arguably, the outcomes reached in this report will be important input for that revision, which is expected to even more increase the already strong alignment between the recommendations of this report and the SIM3 maturity model.

4. Sustainable three-tier maturity approach: how to become a mature team?

The maturity of a CSIRT can only grow by performing the tasks assigned to the team combined with a culture of continuous improvement, supported by proper education and training. Also, policies, procedures and workflows that support the team's goals and tasks, must be in place and need to have been polished by real life application. As all of that, and more, is required in order to be considered a mature team, this clearly requires that the team has been operating long enough to allow that kind of reliance on their own merits.

The question that comes up is: what all is needed to become a mature team?

This chapter will answer this question and provide a process that enables each team – both experienced and new ones – to set and reach their maturity goals over time.

4.1 Applicability and Requirements

What we have considered so far does in fact apply to many types of CSIRTs. To increase maturity has become an essential requirement for capacity building, and for a reliable and proven cooperation between teams.

Clearly, all teams that operate on a national scale or with a national scope, even if only responsible for one sector, need to be mature enough to be reliable partners in the CSIRT cooperation. This is especially true for those teams that have been assigned the role of national CSIRT, designated CSIRT or defined point of contact according to the NISD. But also, any government and military teams including those on the state level within federated structures can be expected to adhere to the same principles.

In all cases it is essential that the teams to which these considerations apply, are well integrated in the existing CSIRT communities. Some of the teams are by definition part of the CSIRT network established by the NISD, but this network is not open to all CSIRTs and it covers only a small part of the globally active teams. Accreditation by TF-CSIRT / Trusted Introducer inside Europe, and FIRST membership globally, are therefore considered evolutionary steps for teams in increasing their maturity. In addition, especially teams with a national scope or role, must be active and supportive members of their national CSIRT community, as this is laying the foundation for a trusted and reliable CSIRT co-operation inside any given country.

4.2 Introducing levels of maturity

As stated in the introduction, it is important to achieve a gradual improvement of operational experience of teams and their maturity. Depending on the team's budget, and on the resources dedicated to establishing maturity, the speed with which different teams manage to reach the desired level of reliability will vary. Other factors like the experience of the staff, the turn-over rate of staff members and the budget attributed to trainings and exercises, are important too as much of the operational excellence of any team resides in their staff.

Past experience has shown that the number of different parameters can be overwhelming, especially for new teams that are planning to prepare for maturity or are limited in the budget available for improvement, while handling day-to-day business and responding to incidents of national interest. To overcome this uncertainty and provide for a maturity program allowing the teams to advance in their own speed but while doing so addressing the most important issues first, we introduce three levels of maturity:

- **Basic Maturity Level** – For this level, activities on all parameters have been started with a clear focus on the mandate and other formal considerations of the team's role. Approximately 80% of the organisational parameters have already been addressed to such a degree, that they can be considered "advanced".

- **Intermediate Maturity Level** – Based on the work done so far, progress for all parameters, except for those already on "advanced" level, has been achieved. Overall, approximately 50% of the human, tool and process parameters can be considered "advanced".

- **Advanced Maturity Level** – The final step directs the efforts to the remaining parameters and achieves a level that is considered "advanced".

As we will explain, the demands for maturity for teams co-operating in the CSIRT Network as defined by the NIS Directive is somewhat higher than for the current Trusted Introducer (TI) Certification [10]. This implies that all teams that are on the "advanced maturity level" can become a TI certified team by applying for it. Due to the set-up of the TI Certification, which is based on a formal process with independent assessments, this may still cause some effort – but this should be limited, as the content covered and the ratings applied are the same.

Assuming that all teams to be considered have already been accredited by the TI, we have used this as the starting point and will focus on the additional efforts to reach the next levels. In the following sections we will examine the four areas of parameters – Organisation, Human, Tools, Processes – for each of the three maturity levels. At the start of each sub-section a table will show the requirements in colour coding. The table below shows an example:

	X-1	X-2	X-3	X-4
Basic	3	3	1	1
Intermediate	4	3	1	2

The previous/current level in this example is "Basic", the desired level is "Intermediate". Already at "Basic" level, the parameter X-2 is on the "Advanced" level, indicated by the dark blue background and white font. All other parameters from the previous/current level have a light background and black font.

In order to advance to the next level "Intermediate", the team needs to substantiate the level for the factors X-1, X-3 and X-4. Three different colours are used here to differentiate:

- Parameter X-1 is pushed to the "Advanced" level, indicated by the dark blue background and white font.
- Parameter X-3 stays on the same level and does not require further work. Therefore, the light background and black font are used for this as before, indicating "no change".
- Parameter X-4 improves, but not yet to "Advanced" level, shown by the light blue background and black font.

4.3 Maturity Level: Basic – how to get the basics right

Specific organisational decisions are necessary with the creation of any new CSIRT. But such decisions are most important if national CSIRTs are set up according to the NIS Directive. Therefore, the focus of reaching the Basic Maturity Level lies on these parameters. But as it is not enough to produce the proper documentation and organisational set-up, work on the other parameters will start.

4.3.1 Basic Maturity Level : Why

For the CSIRT network to function at a basic level covering at least the co-ordinated handling of incidents, it is necessary that the CSIRTs involved have a minimum foundation in terms of their existence (mandate etc.), are reachable and have a basic incident handling process. The Basic Maturity Level focuses on achieving this. The organisational parameters will already reach a fair level of maturity (mostly 3) with this level, while the majority of the other parameters are only level 1 or 2.

As starting point to reach Basic Maturity Level, we use the TI accreditation.[2] This system which has existed for 15 years in Europe, provides a minimal baseline for information that teams should make accessible to other community members in regard their organisation and operation. We found that, within the EU realm, more than 90% of all national CSIRTs or government teams with national scope have already been accredited. This shows that the TI accreditation is well accepted and has indeed become a best practice in and of itself. Compared to other baselines like FIRST membership, the TI accreditation is fully documented and transparent for all participants. It does not rely on a subjective site visit which is carried out in very different ways determined only by the visiting team vouching for the visited team, as happens for FIRST membership. Considering all this, the TI Accreditation provides the deterministic and uniquely shared common viewpoint that serves as the best point to start from.

4.3.2 Organisational Parameters

To provide the foundation of a reliable service, the following organisational parameters need to be documented for external consumption and approved/set into force by the team management. Without this no defined basis for the team’s mission would be available:

- O-1: Mandate
- O-2: Constituency
- O-3: Authority
- O-4: Responsibility
- O-5: Service Description
- O-7: Service Level Description
- O-9: Participation in existing CERT Frameworks
- O-10: Organisational Framework

The parameters O-7 and O-10 will not require further work, as it is not expected that all Service Levels will be actively assessed by higher management, and the Organisational Framework – most often referred to as “CSIRT Handbook” – is not designated to be necessarily published or become widely distributed. Both factors however require to be enforced internally by the team management.

[2] https://www.trusted-introducer.org/processes/accreditation.html

For the two remaining parameters at least some consensus on the team level has to be reached. While it seems rather unlikely that this will not require some sort of documentation to be used consistently such requirements have been postponed to further levels.

- O-8: Incident Classification
- O-11: Security Policy

The table shows an overview of the initial values and the required improvements:[3]

	O-1	O-2	O-3	O-4	O-5	O-7	O-8	O-9	O-10	O-11
Accreditation	**(3)**	**(3)**	**Opt.**	**Opt.**	**Opt.**	**Opt.**	**--**	**(3)**	**--**	**--**
Basic	**3**	**3**	**3**	**3**	**3**	**3**	**1**	**3**	**3**	**1**

4.3.3 Human Parameters

To start the work on those parameters associated with the human workforce three parameters need to be documented for the team itself:

- H-1: Code of Conduct/Practice/Ethics
- H-2: Personal Resilience
- H-7: External Networking

Four parameters are considered for later progress, although certainly many teams will choose to invest in training right from the start and skillset descriptions are often required as part of the employment process anyway:

- H-3: Skillset Description
- H-4: Internal Training
- H-5: External Technical Training
- H-6: External Communication Training

The table shows an overview of the initial values and the required improvements:

	H-1	H-2	H-3	H-4	H-5	H-6	H-7
Accreditation	**should**	**--**	**--**	**--**	**--**	**--**	**should**
Basic	**2**	**2**	**1**	**1**	**1**	**1**	**2**

4.3.4 Tools Parameters

The advancement for most tool related parameters are considered to be addressed in succeeding levels:

- T-2: Information Sources List
- T-3: Consolidated E-Mail System
- T-4: Incident Tracking System
- T-5: Resilient Phone
- T-6: Resilient E-Mail

[3] The parameter O-6 is omitted by intention as this parameter was removed in the early days of the SIM3 development.

- T-7: Resilient Internet Access
- T-10: Incident Resolution Toolset

Three parameters will not require additional work although such is certainly recommended in order to provide a better service in relation to IT Resources (asset management: list of hardware and software used, with versions) used within the constituency and provide better support for the prevention and detection of (some types of) incidents:

- T-1: IT Resources List
- T-8: Incident Prevention Toolset
- T-9: Incident Detection Toolset

The table shows an overview of the initial values and the required improvements:

	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10
Accreditation	--	--	--	--	--	--	--	--	--	--
Basic	1	1	1	1	1	1	1	1	1	1

4.3.5 Process Parameters

Despite the need for many processes there is one process which is mandatory for all teams. Certainly the escalation to the governance level needs to be well documented for external consumption and approved/set into force by the team management:

- P-1: Escalation to Governance level

Documentation is also required for five other parameters, although not yet for external consumption:

- P-8: Process of active team assessment by higher management
- P-9: Emergency Reachability Process
- P-10: Common Mailbox Names
- P-11: Secure Information Handling Process
- P-14: Reporting Process

All other process related parameters are considered to be addressed in succeeding levels:

- P-2: Press Escalation
- P-3: Legal Escalation
- P-4: Incident Prevention Process
- P-5: Incident Detection Process
- P-6: Incident Resolution Process
- P-7: Specific Incident Processes
- P-12: Information Sources Process
- P-13: Outreach Process
- P-15: Statistics Process
- P-16: Meeting Process
- P-17: Peer-to-Peer Process

The tables show an overview of the initial values and the required improvements:

	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10
Accreditation	--	--	--	--	--	--	--	--	--	--
Basic	3	1	1	1	1	1	1	2	2	2

	P-11	P-12	P-13	P-14	P-15	P-16	P-17
Accreditation	--	--	--	--	--	--	--
Basic	2	1	1	2	1	1	1

4.4 Maturity Level: Intermediate – how to advance

Based on the basis achieved by the previous efforts, the main focus now is to set up the management control functions for the organisational parameters, pushing 8 of 10 parameters to the "Advanced" level. The work on the other areas – Human, Tool, Process – is building on the previous work and ensures progress on most parameters.

4.4.1 Intermediate Maturity Level : Why

For the CSIRT network to function reliably in regard the co-ordinated handling of incidents, and also allows additional joint activities (like vulnerability handling), it is necessary that the CSIRTs involved reach a more advanced maturity level than Basic, focusing on a mature foundation and decent descriptions of all relevant tools, processes and human aspects. The Intermediate Maturity Level has been constructed to achieve this. The organisational parameters will now already reach a high level of maturity (more than 50% will be at level 4), the tool parameters will be at level 2, whereas the human and process parameters will be at either level 2 or 3, depending on their relevance for the CSIRT network co-operation.

4.4.2 Organisational Parameters

The "Intermediate" level requires six more organisational parameters to become management controlled. These are:

- O-1: Mandate
- O-2: Constituency
- O-3: Authority
- O-4: Responsibility
- O-5: Service Description
- O-9: Participation in existing CERT Frameworks

For the two remaining parameters for this level documentation is required:

- O-8: Incident Classification
- O-11: Security Policy

The table shows an overview of the initial values and the required improvements:

	O-1	O-2	O-3	O-4	O-5	O-7	O-8	O-9	O-10	O-11
Basic	3	3	3	3	3	3	1	3	3	1
Intermediate	4	4	4	4	4	3	2	4	3	2

4.4.3 Human Parameters

Summarizing the progress for these parameters is easy: advancements for all parameters. To already started work on the documented parameters leads to documents that are documented for external consumption and approved/set into force by the team management:

- H-1: Code of Conduct/Practice/Ethics
- H-2: Personal Resilience
- H-7: External Networking

The other four parameters are now to be documented at least for internal use by the:

- H-3: Skillset Description
- H-4: Internal Training
- H-5: External Technical Training
- H-6: External Communication Training

The table shows an overview of the initial values and the required improvements:

	H-1	H-2	H-3	H-4	H-5	H-6	H-7
Basic	**2**	**2**	**1**	**1**	**1**	**1**	**2**
Intermediate	**3**	**3**	**2**	**2**	**2**	**2**	**3**

4.4.4 Tools Parameters

Progress related to the tool parameters is achieved by providing proper documentation for internal use by the team for:

- T-2: Information Sources List
- T-3: Consolidated E-Mail System
- T-4: Incident Tracking System
- T-5: Resilient Phone
- T-6: Resilient E-Mail
- T-7: Resilient Internet Access

Work on the following parameter is not yet required:

- T-10: Incident Resolution Toolset

The table shows an overview of the initial values and the required improvements:

	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10
Basic	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Intermediate	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**

4.4.5 Process Parameters

Of the five documented (for internal use within the team) parameters only one (P-10: Common Mailbox Names) will not need to be documented for external consumption and approved/set into force by the team management:

- P-8: Process of active team assessment by higher management
- P-9: Emergency Reachability Process
- P-11: Secure Information Handling Process
- P-14: Reporting Process

The majority of not yet documented process related parameters are now considered to be required for internal use by the team:

- P-2: Press Escalation
- P-3: Legal Escalation
- P-4: Incident Prevention Process
- P-5: Incident Detection Process
- P-6: Incident Resolution Process
- P-7: Specific Incident Processes
- P-12: Information Sources Process
- P-13: Outreach Process
- P-15: Statistics Process

The last two processes still handled informally will need to be addressed before moving to the "Advanced" level:

- P-16: Meeting Process
- P-17: Peer-to-Peer Process

The tables show an overview of the initial values and the required improvements:

	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10
Basic	3	1	1	1	1	1	1	2	2	2
Intermediate	3	2	2	2	2	2	2	3	3	2

	P-11	P-12	P-13	P-14	P-15	P-16	P-17
Basic	2	1	1	2	1	1	1
Intermediate	3	2	2	3	2	1	1

4.5 Maturity Level: Advanced – how to reach the objective

While there are only some small efforts left for the organisational parameters by now, the focus of this step is to finish the efforts for the other three areas – Human, Tool, Process – successfully.

4.5.1 Advanced Maturity Level : Why

For the CSIRT network to function excellently in regard the co-ordinated handling of incidents, and also reliably supports additional joint activities like the sharing of threats and early-warning data, vulnerability handling, it is necessary that the CSIRTs involved reach an advanced maturity level, beyond Intermediate, focusing on well described, approved – and in various cases, actively assessed – processes, tools and human aspects. The Advanced Maturity Level has been constructed to achieve this. The organisational parameters were already at a high level with Intermediate, but now also all the human, tool and process parameters will reach level 3, and in important cases even level 4.

Note that the name “Advanced” implies that Certification can take place. This is however outside the scope of this report. The TI Certification is the currently only existing certification scheme for CSIRTs, which is operated by TF-CSIRT/TI in Europe. At this moment, the levels chosen in this report are equal to *or exceed* in several cases the existing Certification demands. This is partially due to the fact that these demands have been drawn up back in 2009, but also to the fact that the NISD invokes some stronger maturity demands. The TF-CSIRT/TI Certification is currently under revision, to be concluded in 2017. It can be expected that some of the demands will become more strict and in fact the standard set in this report is expected to be close to that. In all cases, when a team reaches the Advanced level, and have done their assessment well (see 4.6), it is to be expected that actual TI Certification – where the assessment is done by means of independent, external review, should be within easy reach.

4.5.2 Organisation Parameters

For the final level the two remaining parameters for this level are now made available externally or enforced by the team management:

- O-8: Incident Classification
- O-11: Security Policy

The table shows an overview of the initial values and the required improvements:

	O-1	O-2	O-3	O-4	O-5	O-7	O-8	O-9	O-10	O-11
Intermediate	4	4	4	4	4	3	2	4	3	2
Advanced	4	4	4	4	4	3	3	4	3	3

4.5.3 Human Parameters

Only the four parameters that until now have been required only to be documented for internal use have to be improved. For the “Advanced” level they are required to be made available externally or enforced by the team management:

- H-3: Skillset Description
- H-4: Internal Training
- H-5: External Technical Training
- H-6: External Communication Training

The table shows an overview of the initial values and the required improvements:

	H-1	H-2	H-3	H-4	H-5	H-6	H-7
Intermediate	3	3	2	2	2	2	3
Advanced	3	3	3	3	3	3	3

4.5.4 Tools Parameters

Based on the proper documentation for internal use by the team produced at least for the “Intermediate” level the “Advanced” level requires now documents that are made available externally or enforced by the team management:

- T-2: Information Sources List
- T-3: Consolidated E-Mail System
- T-4: Incident Tracking System

- T-5: Resilient Phone
- T-6: Resilient E-Mail
- T-7: Resilient Internet Access

Work on the following parameter is also concluded by now resulting in the proper documentation:

- T-10: Incident Resolution Toolset

The table shows an overview of the initial values and the required improvements:

	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10
Intermediate	1	2	2	2	2	2	2	1	1	1
Advanced	1	3	3	3	3	3	3	1	1	2

4.5.5 Process Parameters

Two of the process parameters are considered to be of overriding importance for the perception and success of the team's operation. One describes the system by which the higher management actively assesses the team, the other ensures the continuous improvement of the team's operations. In addition the reporting allowing the monitoring of the team's performance as well as the assessment of current trends and developments are key requirements. Both parameters therefore need to become enforced or examined by an entity overseeing the team's operation:

- P-8: Review / Feedback Processes
- P-14: Reporting Process

Of those parameters, that had been documented for internal use by the team the following six are now required to be documented for external consumption and approved/set into force by the team management:

- P-2: Press Escalation
- P-3: Legal Escalation
- P-7: Specific Incident Processes
- P-12: Information Sources Process
- P-13: Outreach Process
- P-15: Statistics Process

The last two processes still handled informally will need to be at least documented for internal use by the team:

- P-16: Meeting Process
- P-17: Peer-to-Peer Process

The tables show an overview of the initial values and the required improvements:

	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10
Intermediate	3	2	2	2	2	2	2	3	3	2
Advanced	3	3	3	2	2	2	3	4	3	2

	P-11	P-12	P-13	P-14	P-15	P-16	P-17

Intermediate	3	2	2	3	2	1	1
Advanced	3	3	3	4	3	2	2

4.6 Assessment

With any scheme established to allow a common approach towards increasing maturity, there needs to be some mechanism to exchange related status information, and to ensure within the trust group accepting those maturity levels, that such status information can be relied upon. Within the CSIRT communities, specific "trust marks" have already been established, but it is certain that this new process supporting the described maturity levels will establish another "trust mark", as it builds on the existing maturity assessment system (SIM3) yet comes with higher demands for national teams with critical tasks.

For this reason, it is necessary to define some kind of assessment that supports the new trust mark but is anchored in the community itself. Two approaches that can be combined are recommended:

1. **Self-Assessment –** The SIM3 maturity model has been created as a model for self-assessments, recognizing the basis needs for each team itself to determine its own level of success in advancing to a more reliable and mature service-oriented entity.

2. **Peer Review –** By documenting the outcome of any self-assessment in a more formal and structured document, the outcome authorized by the team's management can be exchanged within the trusted community. By exchanging this information, the team exposes itself but it does so to demonstrate that trust can be placed on it.

As it was explained throughout this document there are limits that can be achieved by self-declaration. It became obvious that requirements related to some parameters need to be assessed not by the team itself but in an independent fashion. It is clear therefore, that the outcome of any self-assessment cannot demonstrate in an objective way towards other teams that such an independent assessment is indeed in place and functional. To overcome this gap, the peer review is an important step forward, even if not the whole answer.

It is proposed that for all parameters requiring active assessment (level 4) the team needs to provide evidence to its peers – the other teams – supporting the claim. If the claim is checked and approved, this result can be recorded as part of the available status information.

4.7 Proposed Timeline

As said in the introduction of this chapter it will take some time to advance to a mature team. Due to the reasons described maturity cannot be achieved by the simple will of anyone. You might compare it to the situation of young people getting their driving license: They (finally) got the mandate/license and passed all tests, so operationally they can drive and there is a justifiable hope that they will not do harm to others or themselves. But others would not consider any such person a "mature" driver. For that much more practice and experience is needed, enabling us to drive safely despite conditions that might be far from optimal. The same is true for advancing to be a "mature" team.

Before you start

- Stock taking
- Self-check / self-assessment
- Membership in FIRST and applicable national CSIRT communities; accreditation by TI
- Staff, budget
- Official announcement, recognition by the government / authorities

Reaching basic level

While with the core elements in place a lot of questions are answered already the ground rules are laid out. These needs to be documented, communicated and aligned to the operational context and conditions enforced by other circumstances like the ability to provide physical security, etc.

We propose that national teams in the NISD context take up to a year to reach the basic level. Teams that have been accredited by TF-CSIRT/TI will usually be beyond the Basic Maturity Level and should be close to the Intermediate Maturity Level.

Progressing to intermediate level

Given the preparation taken until now it is expected that the intermediate level can be reached by focusing on the internal processes and tools including training of the staff members.

We propose that national teams in the NISD context take up to 2 years (after reaching basic level) to reach the intermediate level. Teams that have been certified by TF-CSIRT/TI should already be on this level.

Advancing to advanced level

The final steps are usually taking more time than expected: “the devil is in the detail”.

We propose that national teams in the NISD context take up to 2 years (after reaching intermediate level) to reach the advanced level.

Conclusion

It is expected that some steps might take longer than others, but extending all levels to the maximum allowed time period is not in the interest of providing a network of mature and settled teams. Therefore, an overall maximum of 5 years to become a advanced team – counting from the official announcement of an applicable role – is defined as baseline requirement.

4.8 Overview of Maturity Levels and Requirements

Annex A summarises the three maturity levels and the individual requirements for each parameter.

5. Conclusions

The NISD aims at creating a CSIRT Network “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation”. Each Member State shall designate one or more CSIRTs that shall comply with a set of defined high-level requirements.

What that means for the maturity of national CSIRTs has been researched in this study, with the following conclusions:

1. A sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NIS Directive.
2. The three-tier approach towards maturity levels that ENISA adopted in the 2013 report ‘CERT community - Recognition mechanisms and schemes’ can be used to define three levels when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and advanced.
3. A specific definition of those three levels for the benefit of the NISD CSIRT Network has been proposed in this report: essentially a set of requirements, defined on three levels of maturity. Basic level already allows successful co-operation between teams on incident handling, the higher levels are needed to allow the members of the CSIRT network to interact on all levels, including pro-actively. The Advanced level has been defined at the level of the existing CSIRT Certification scheme in Europe, which means that certification is within reach once that maturity level has been reached.
4. A validation process based on self-assessments and peer-reviews has been proposed in this report.

By adopting the proposed approach, the NISD CSIRT Network will have immediate access to a clearly defined CSIRT maturity improvement process that is both implementable and sustainable. A growth path is suggested here that asks teams to reach basic level within one year, intermediate two years later and advanced another two years later: a total of five years maximum.

References

[1] http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement/

[2] https://www.enisa.europa.eu/publications/csirt-capabilities (2015)

[3] https://www.enisa.europa.eu/publications/cert-community-recognition-mechanisms-and-schemes (2013)

[4] https://www.trusted-introducer.org/SIM3-Reference-Model.pdf (2009)

[5] https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts & https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities & https://www.enisa.europa.eu/publications/baseline-capabilities-for-national-governmental-certs & https://www.enisa.europa.eu/publications/baseline-capabilities-of-national-governmental-certs-policy-recommendations

[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[7] https://check.ncsc.nl/static/CSIRT_MK_guide.pdf (2015)

[8] The Nippon CSIRT Association (NCA: see http://www.nca.gr.jp/en/index.html) is the co-operation body of over 100 CSIRTs in Japan. Several NCA members use SIM3 and the NCA has evaluated their use. Their comments and recommendations were shared in private communication with the authors of this study.

[9] http://www.first.org/membership/site-visit-v2.0.pdf (2006-2013)

[10] https://www.trusted-introducer.org/processes/certification.html

ANNEX A: Overview of Maturity Levels and Requirements

The tables below summarize the three levels and show the individual requirements for each parameter.

Organisation Parameters

	O-1	O-2	O-3	O-4	O-5	O-7	O-8	O-9	O-10	O-11
Basic	3	3	3	3	3	3	1	3	3	1
Intermediate	4	4	4	4	4	3	2	4	3	2
Advanced	4	4	4	4	4	3	3	4	3	3

Human Parameters

	H-1	H-2	H-3	H-4	H-5	H-6	H-7
Basic	2	2	1	1	1	1	2
Intermediate	3	3	2	2	2	2	3
Advanced	3	3	3	3	3	3	3

Tools Parameters

	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10
Basic	1	1	1	1	1	1	1	1	1	1
Intermediate	1	2	2	2	2	2	2	1	1	1
Advanced	1	3	3	3	3	3	3	1	1	2

Process Parameters

	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10
Basic	3	1	1	1	1	1	1	2	2	2
Intermediate	3	2	2	2	2	2	2	3	3	2
Advanced	3	3	3	2	2	2	3	4	3	2

	P-11	P-12	P-13	P-14	P-15	P-16	P-17
Basic	2	1	1	2	1	1	1
Intermediate	3	2	2	3	2	1	1
Advanced	3	3	3	4	3	2	2

ENISA
European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

Heraklion Office
Nikolaou Plastira 95
Vassilika Vouton, 700 13, Heraklion, Greece

TP-03-19-319-EN-N

1 Vasilissis Sofias, Marousi 151 24, Athens, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-292-9
DOI: 10.2824/860039