Global CSIRT Maturity Framework

Stimulating the development and maturity enhancement of national CSIRTs

Version 2.0 | April 2021

Global CSIRT Maturity Framework

Stimulating the development and maturity enhancement of national CSIRTs

Authors: Hanneke Duijnhoven (TNO), Tom van Schie (TNO) and Don Stikvoort (m7)

Management Summary

The Global CSIRT Maturity Framework is intended to contribute to the enhancement of global cyber incident management capacity, with a focus on national CSIRTs. Cyber incidents and developments are inherently transnational and effective response is dependent upon transnational collaboration. The establishment of national CSIRTs is an essential step to facilitate cyber capacity building both within and across nations and make it more effective. The Global CSIRT Maturity Framework is aimed at parties involved in planning, building and leading such capacities.

The Global CSIRT Maturity Framework includes a well-established maturity model, as well as an elaboration of pre-defined maturity stages that can be used as a guideline for steps towards increased maturity, completed with practical guidance on how to work with the maturity model at different phases – from pre-establishment to advanced stages of maturity. It is important to recognise that the framework is not intended to be prescriptive, but is meant to support and stimulate national efforts on building and improving cyber incident response capacity. However, the maturity stages that have been defined are based on extensive experience and expertise in the CSIRT community and offer valuable guidance for national CSIRTs in regard the quality level to aspire to. The Global CSIRT Maturity Framework combines previous models that are widely recognised and adopted. In particular, the Open CSIRT Foundation SIM3 model and the European Union Network and Information Security Agency (ENISA) three-tier maturity approach are used as a basis for this Global CSIRT Maturity Framework for national CSIRTs.

The updated version 2.0 includes more in-depth information and explanation about the relevance of different parameters of the maturity model for national CSIRTs.

Contents

Introduction

This document presents a CSIRT Maturity Framework that is intended to contribute to the enhancement of global cyber incident management capacity, with a focus on national CSIRTs.[1] It is aimed at parties involved in planning, building and leading such capacities. The importance of establishing national incident response capacity is highlighted by institutions such as the UN Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International Security (UN GGE), the International Telecommunication Union (ITU) and by regional organisations such as the Organisations of American States (OAS), Commonwealth Telecommunications Organisation (CTO), and the European Union (EU) [1]. This document has been developed in the context of the Global Forum on Cyber Expertise (GFCE), which seeks to stimulate, develop and enhance practical initiatives to build and strengthen cyber capacity. The GFCE Global Good Practice on National CSIRTs [2] stresses the importance of national Computer Security Incident Response Teams (CSIRTs) in building effective capacity to prevent, react promptly, and recover quickly from cyber incidents at the national level. Furthermore, national CSIRTs play a crucial role in the collaboration and coordination between national and international communities and organisations. Cyber incidents and developments are inherently transnational and effective response is dependent upon transnational collaboration. The establishment of national CSIRTs is an essential step to facilitate and coordinate cyber capacity building both within and across nations.

Within the CSIRT community incident management is generally defined as the combination of incident prevention, detection, resolution and quality management – thus much more than just incident handling. Thus, CSIRTs form an essential element of cyber incident management and cyber capacity in general.

The concept of CSIRTs emerged from collaborative experiences gained by organisations starting with the response to the 'Internet worm' which hit the Internet on the 2nd of November 1988 [3]. The first computer incident response teams were established mostly by academic communities. Over time, the need and value of CSIRTs has become clear to non-academic communities too. Currently, CSIRTs exist at all levels of public and private

[1] This document uses the term 'national CSIRTs' to refer to a range of national cyber (coordination and response) activities, including CIIP and governmental teams. Depending on the context, a national CSIRT can have a different focus or name.

organisations and businesses (e.g. individual organisations, IT and industrial control system manufacturers or vendors, sectors, governments, nations and international organisations).

Internal CSIRTs (sometimes also referred to as “enterprise” CSIRTs) operate at the level of individual organisations – this can be any type of organisation, such as a private company, multinational, not-for-profit, university, hospital, government agency. Such internal teams have a clear mandate and knowledge to perform hands-on incident management activities within an organisation’s network of IT systems. Another type of CSIRTs has an external focus and provide their services to a sector, or nation, and usually have limited mandate to access or implement security measures within the actual IT systems of their constituency. Therefore, these focus more on coordination of response, the analysis of threats and incidents, and other forms of support to members within the constituency.

National CSIRTs are in the latter category. They generally provide the capability of rapid, integrated and coordinated cyber incident response for national sectors, cyber dependent communities such as e-commerce enterprises or financial institutions, critical infrastructure and the nation at large, as well as being important linking pins in the global CSIRT community. Depending on the specific legal and political context, national CSIRTs can have a variety of focus areas and mandates. In some nations, national CSIRT are institutionally embedded in (or closely related to) a national cyber security centre (NCSC) or similar authority or agency. NCSCs have a broader mandate as national coordination centres; they provide technical and policy expertise and are usually tasked with executing national crisis exercises and contributing to technical standards and legislation. In some countries, national CSIRT functions are distributed between two, or even more, teams. In case of multiple national teams, it is important that the mandate and constituencies for each team are clearly defined and that they can cooperate closely.

Table 1 displays examples (non-exhaustive) of different institutional embedding of national CSIRTs across the globe. For more examples, see for instance the list of national teams maintained by CERT/CC as part of their NatCSIRT initiative [4].

Table 1 - Examples of National CSIRTs embedded in different ways

National CSIRT institutional embedding as part of:	Examples
Prime Minister's office	CERT VU (Vanuatu), CERT-BE (Belgium)
Agency under supervision of a ministry (Interior, ICT, Environment et al.)	ThaiCERT (Thailand), CERT-GH (Ghana), CERT Tonga (Tonga)
Communications regulatory authority	TZ-CERT (Tanzania), NCSC-FI (Finland), CARICERT (Curaçao)
National security authorities	TTCSIRT (Trinidad & Tobago)
National defence	Hellenic CSIRT (Greece)
Cyber security agency	SingCERT (Singapore), CERT-SA (Saudi Arabia)
National Cyber Security Centre (NCSC)	NCSC (New Zealand), Canadian Centre for Cyber Security (Canada), NCSC-NL (The Netherlands)
Domain name registrar	CERT.br (Brazil), CERT.at (Austria)
Private limited liability	Sri Lanka CERT|CC (Sri Lanka), BruCERT (Brunei)

Encouraging the establishment, expansion and maturity of national CSIRTs worldwide contributes to the ambition of building global cyber capacity, supplementing the existing network of private industry and academic/research CSIRTs. To do so, it is important to approach the development of this network both from a technical as well as a policy perspective. Existing models and good practices for CSIRTs and CSIRT maturity not only can support nations that are ready to establish a national CSIRT, but also nations that want to enhance the maturity of their national team. The Global CSIRT Maturity Framework presented here includes a maturity model, an elaboration of pre-defined maturity stages that can be used as a guideline for steps towards increased maturity and practical guidance on how to work with the maturity model at different phases (from pre-establishment through maturity assessment). It is important to recognise that the framework is not intended to be prescriptive, but is meant to support and stimulate national efforts on building global cyber incident response capacity. However, the maturity stages that have been defined are based on extensive experience and expertise in the CSIRT community and offer valuable guidance for national CSIRTs in regard to the quality level to aspire to.

The Global CSIRT Maturity Framework combines previous models that are widely recognised and adopted. In particular, the Open CSIRT Foundation SIM3 model [5] and the European Union Network and Information Security Agency (ENISA) three-tier maturity approach [6] are used as a basis for this CSIRT Maturity Framework for national CSIRTs:

Open CSIRT Foundation (OCF) – SIM3

SIM3 is designed as a generic maturity model that applies to all types of CSIRTs, including national CSIRTs [5]. The OCF encourages the Global Forum on Cyber Expertise members to use the current SIM3 version, under the condition that it is used unchanged and with the request that any potential improvements of SIM3 are shared with the OCF in order to help improve SIM3.

ENISA – CSIRT three-tier maturity approach

The ENISA CSIRT three-tier maturity approach is based on SIM3 and was developed to support the maturity development of national CSIRTs in the EU [6]. This staged maturity approach is globally applicable. ENISA has given the GFCE community permission to use their three-tier maturity approach, under the condition that it is used as much as possible in its original form and that any potential changes are fed back to ENISA.

The choice to adopt these existing models is based on a review of available CSIRT models looking at their global applicability for the development of national CSIRTs. In addition, elements of the FIRST CSIRT Services Framework [7] and several other existing models are adopted.

In the next section the maturity model and the maturity stages are presented. The final section of the document contains practical guidelines for working with the Maturity Framework.

The Global CSIRT Maturity Framework

At the core of the Global CSIRT Maturity Framework lies the maturity model SIM3 [5] as well as ENISA's CSIRT three-tier maturity approach [6]. In this chapter both the maturity model and ENISA's three maturity stages are presented, in such a way that they can be applied globally.

Security Incident Management Maturity Model (SIM3)

SIM3 stands for Security Incident Management Maturity Model and has been in use since 2009[2]. The maturity model has been applied by teams all over the world, including various national CSIRTs[3]. In the European Union, national CSIRTs are encouraged to develop their maturity using the ENISA CSIRT three-tier maturity approach which is based on SIM3.

SIM3 features 44 parameters. Parameters are attributes relevant for either the organisation, operationalisation or functioning of a CSIRT.

The SIM3 parameters are divided over 4 categories:

O: Organisational

The organisational ('O') parameters focus on aspects that together describe the foundation and extent of the CSIRT's activities (i.e. the mandate, setup and services of the CSIRT, and the framework connecting all organisational aspects).

H: Human

The human ('H') parameters in the framework focus on important aspects related to the CSIRT staff (this is not only about technical staff, but for staff members). Together, these parameters reflect how the team views its staff in relation to the work of the team and how this is organised.

SIM3 Applications

TF-CSIRT, the European CSIRT cooperation, has used SIM3 since 2010 for an optional Certification of their Accredited members. 25 teams have been Certified until March 2019, 7 of which are national teams [13].

The Nippon CSIRT Association (NCA), the Japanese cooperation society for over 300 CSIRTs, uses SIM3 for improving the maturity of their members [8].

ENISA adopted SIM3 as the starting point for their staged maturity approach for EU CSIRTs Network members [6].

FIRST is working on taking up SIM3 as part of their membership framework [9].

[2] The Open CSIRT Foundation (OCF) governs and maintains SIM3, and trains and certifies SIM3 auditors [5].
[3] Two online measurement tools exist. The OCF tool aims at all sorts of CSIRTs worldwide, including national ones [11]. ENISA's tool aims at national CSIRTs [12].

T: Tools

The tools ('T') parameters refer to the tools and technologies that are used by the CSIRT to reach its objectives and offer the services to their constituency. A 'tool' in this context can be a list, an excel sheet or in most advanced cases an actual implementation of advanced tooling.

P: Processes

The processes ('P') parameters focus on a set of processes that should be well organised in order for a CSIRT to perform its tasks. The word 'process' is meant in a generic way – it includes not only processes in the sense of a logical set of sequential/parallel steps, but also policies, both of the more fundamental kind as well as very basic policies. Some of the Process parameters are connected with parameters from the other areas (Organisation, Human, and Tools), where the description or list is more in those other areas, and the P-parameters focus on the steps that need to be taken.

The 44 parameters are listed in Table 2 below. The full details for all parameters are given in Appendix A.

Table 2- Overview of SIM3 parameters

Parameter number	Parameter description	Parameter number	Parameter description
O-1	Mandate	T-6	Resilient E-Mail
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-7	Service Level Description	P-1	Escalation to Governance Level
O-8	Incident Classification	P-2	Escalation to Press Function
O-9	Integration in existing CSIRT Systems	P-3	Escalation to Legal Function
O-10	Organisational Framework	P-4	Incident Prevention Process
O-11	Security Policy	P-5	Incident Detection Process
H-1	Code of Conduct/Practice/Ethics	P-6	Incident Resolution Process
H-2	Personnel Resilience	P-7	Specific Incident Processes
H-3	Skillset Description	P-8	Audit/Feedback Process
H-4	Internal Training	P-9	Emergency Reachability Process
H-5	External Technical Training	P-10	Best Practice E-mail and Web Presence
H-6	(External) Communication Training	P-11	Secure Information Handling Process
H-7	External Networking	P-12	Information Sources Process
T-1	IT Resources List	P-13	Outreach Process
T-2	Information Sources List	P-14	Reporting Process
T-3	Consolidated E-Mail System	P-15	Statistics Process
T-4	Incident Tracking System	P-16	Meeting Process
T-5	Resilient Phone	P-17	Peer-to-Peer Process

When working with the SIM3 framework, each parameter can be measured on a scale of 0 to 4 (see Table 3).

Table 3 – SIM3 parameter measurement scale

Scale	Status	Indicators
0	Not available / undefined / unaware	-
1	Implicit	Known/considered but not written down, 'between the ears', 'tribal knowledge'
2	Explicit, internal	Written down but not formally adopted or reviewed
3	Explicit, formalised on authority of CSIRT head	Approved or published
4	Explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis	Subject to a control process and/or review

To use this measurement scale appropriately, some additional explanation about each of the five levels (what they mean and what the evidence procedure could be) may be helpful:

LEVEL 0 "Not available / undefined / unaware"

This score is mostly only met with teams who are fairly novice, as it means that the team members *have not even been thinking yet* about the parameter in question. If during an assessment or audit all attendants produce blank looks when a parameter is mentioned, this may be a candidate for level 0. When a team starts actively discussing a parameter, there is a high likelihood of it moving to level 1 fairly soon.

LEVEL 1 "Implicit"

This score is typically encountered with novice teams but, for some parameters, also with experienced teams where a few experts know how to do things but never took the trouble of writing them down. When doing an assessment or audit and a parameter at level 1 is encountered, it is worthwhile asking a few team members to explain how they think about that parameter. Chances are that the explanations will be different enough to convince the team as well as the team management that it would be a good idea to actually write the content for this parameter down, as to increase consistency within the team – and also making it easier to get new team members up to speed.

LEVEL 2 "Explicit, internal"

This score is typically encountered when teams have internal information systems of a more informal type. Like a team-wiki, or a shared site or similar. It is strongly recommended to have a facility like that for any CSIRT as it allows an easy way to bring the most important processes, tools (and manuals) and policies under the direct attention of those doing the incident management work. A wiki-style approach has the added advantage of allowing hyperlinks, thus enabling the internal information to be easily structured and interconnected: example, T-2 is the information sources list, and from that list you could easily point at the process(es) relevant for those various sources – and those processes comprise the P-12 parameter.

There are also some other cases than can lead to a level 2 score, like for instance when some tool used by the team holds information relevant for one of the parameters, but this information has not been ratified by the team management. Example: the incident tracking system (T-4) of the team will most likely have some kind of incident classification scheme (O-8) on board – but that will be in the form of a dropdown choice: when that dropdown list has not been formally approved by the team management, the O-8 parameter scores at level 2.

Going back to the wiki-style approach: the typical character of that approach is that various team members can write texts and fit them in – and even when consensus among team members about such texts will come into existence after continued use (and adaptation, again wiki-style), this is still level 2, as there is no formal approval by the team management. Level 2 is certainly valid to begin documentation with, but for most information it is advisable that, at some stage, what has come to be the consensus is also recognised as such and supported by the team management – leading to level 3.

LEVEL 3 "Explicit, formalised on authority of CSIRT head"

This score applies for any parameter where the subject matter of that parameter has been formally and explicitly (in "writing") approved by the team management. To mention a few of the most common situations for level 3:

- The subject matter is part of policy or process documents on the team level, authorised by the team management: these comprise the most simple and direct case, however the risk inherent in *separate* documents is that if there are too many of those the overview is lost and it can become a separate – paper – reality, rather than part of the day-to-day procedures of the team. Therefore, it is important to integrate such documents in team operations and information systems to ensure that team members actually know and use them. For instance by integrating them into a team-wiki or similar. In addition, it is strongly recommended to use an expiry and maintenance system for team-internal documents.

- Relevant policy (or process) documents authorised on a governance level higher than the team management: these are automatically also valid for the team management and the team; however it is essential that they are embedded into the team operations and information systems as to ensure that the team members actually know and use them.
- Wiki-style level 2 information/pages/documents that are "upgraded" to become level 3: this of course requires explicit (visible) authorisation by the team management of such "pages". It is currently not demanded by SIM3 but it is warmly recommend to go one step beyond this and not just do authorisation, but also include some system of expiry and maintenance for such pages. Some wiki-types have facilities or plugins to make that easier.

LEVEL 4 "Explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis"

This score implies level 3 plus an important addition that ensures that the parameter in question is no longer just an internal matter of the team, but has the active attention of some higher governance level, above the team management. There needs to be evidence of this, and the evidence must include the following:

1. There must be a process of checking, assessing or auditing of this parameter on the authority of a higher governance level.
2. This process must be followed regularly. There is currently no set rule for this in SIM3, but as best practice "regular" means *at least* once every 2 years, and usually once per year.
3. The process must be "active", which means in that there is a feedback mechanism towards the team management (and team) in addition to the process of checking and reporting on that. This feedback mechanism is meant to ensure that there is communication about the parameter between team (management) and higher governance levels.

This level 4 mechanism is meant to ensure that (a) the higher level of governance is actively aware of some of the crucial aspects of the nCSIRT and how it functions in real life, and (b) as a consequence, to enable constructive communication between higher governance level and the team in order to enable improvements: clearer policies, better tools and processes, more people, better trainings and education, etc.

The evidence for level 4 is not always clear-cut. The clearest cases are the following two:

- When the topic of a parameter is formally and unambiguously part of the national cyber (security) legislation that parameter automatically scores level 4, because it is assumed that the system of legislation and the checks and balances associated with

that are more than sufficient to warrant a level 4. It is however important to note here that the mere mentioning of something in the law – even if clear and unambiguous – still requires the team to implement this internally as to be able to effectively "make the law work". So this still requires documentation inside the team for such aspects, embedding in a team information system (e.g. team wiki), integration in internal training, etcetera.

- When there is a team organisational framework or charter (O-10) or a "team handbook" it is strongly advised to have a paragraph there about the assessments/audits for the team, which is essentially the P-8 parameter process. This should include internal team assessments (which on their own are not sufficient for level 4) but it should also address the process of auditing the team by a higher governance level or by an auditing department. As such higher level audits usually set their own rules, it is recommended to acknowledge their independent position, but to request a minimum set of aspects (which could directly be translated into SIM3 parameters) on which the team wants to be audited. Most of the O-parameters could be included there, plus optionally some others, like H-2, P-1 and P-2.

In other cases, it is often harder to find clear *evidence* for the level 4 character. For instance, when an auditing department does an extensive audit of the nCSIRT every year, and they do use SIM3 as one of the controlling documents – but no one has written down some minimum requirements for that audit. In such a case, alternative evidence can be a posteriori rather than a priori: meaning, simply ask for a few of those audit reports and see what is in there in order to be able to gauge whether it is reasonable to assume that certain SIM3 parameter is indeed audited in the level 4 way (including feedback to the team) and therefore there is reasonable substantiation for level 4.

Figure 1 shows a (hypothetical) result of a CSIRT maturity assessment. The 44 parameters are given a score and the figure provides visual insight in the maturity of a team.

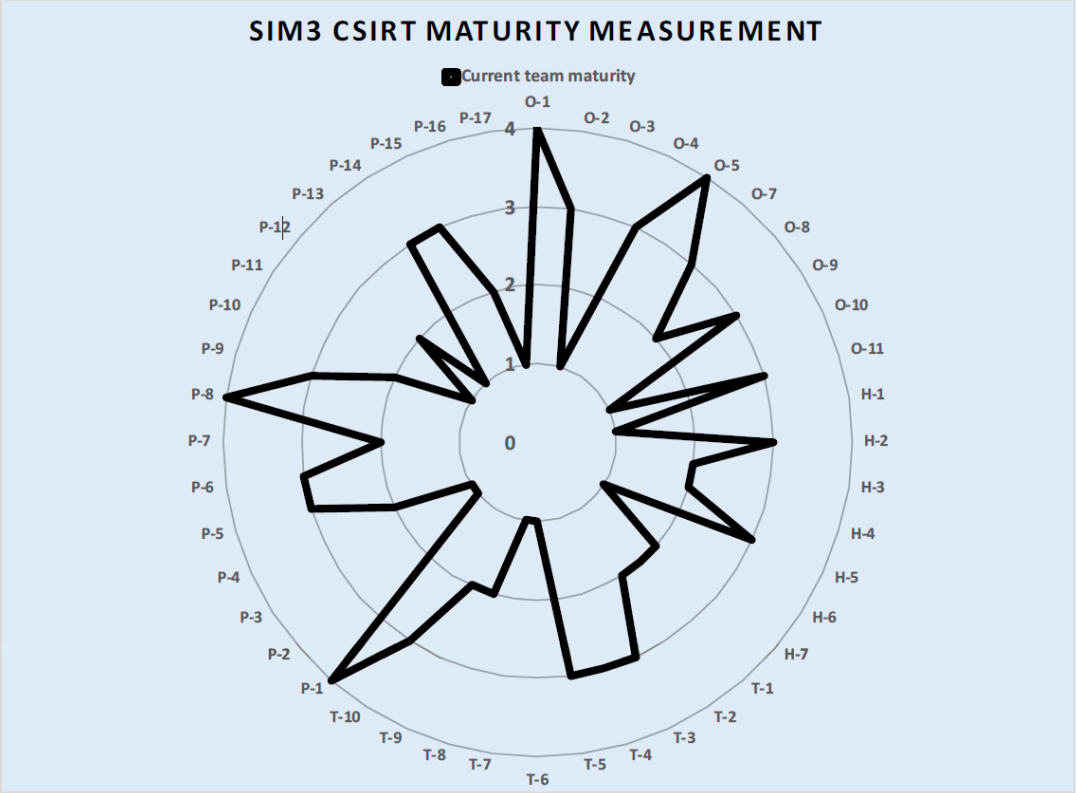


Figure 1: CSIRT maturity assessment example outcome

CSIRT Maturity stages

This paragraph provides information on the maturity stages that can be used to assess the maturity of a national CSIRT and to support the decision-making process on where to focus effort to increase maturity. The maturity stages are adopted from the three-tier maturity approach that ENISA developed [6]. Three stages are described: *basic*, *intermediate* and *advanced*. For each stage a minimum value is assigned for each of the 44 parameters. The values for each parameter at each of the three stages are based specifically on the profile requirements for most national CSIRTs. This means that some parameters are more relevant for national teams than others.

National CSIRTS, by virtue of their *national* responsibility, should always be mandated by the government or through legislation to legitimately fulfil their national role. This also reflects on many of the other aspects related to the scope of their activities. For this reason, even at the Basic stage nCSIRTs should obtain relatively high levels of maturity on many of the O-parameters. In turn, the aspects addressed by the H-parameters are usually part of the internal management processes of the team and do not necessarily require regular control from governance levels above the CSIRT management. This means that for the three maturity

stages for nCSIRTs, none of these parameters require a level higher than 3. Of course it is possible that in some countries, there will be a conceived need to have auditing and feedback from a higher level of governance on for instance the availability of sufficient staff (parameter H-2) or to help ensure they are properly educated (parameters H-4 to H-6) – and that could be a reason for a level 4 for these parameters – but in general such a level is not required for the three maturity stages for national CSIRTs. As a final example, most national CSIRTs will play less of a role in actual incident prevention and therefore the value for T-8 (Incident prevention toolset) and P-4 (Incident prevention process) are low across all three maturity stages. Appendix A provides a more in-depth explanation of the relevance of each of the 44 parameters for national CSIRTs.

The *basic* and *advanced* stages allow for national CSIRTs to define a growth path. New teams can first aim to achieve the *basic* stage at relatively short term, as this is really the starting point for any national team, and also provides the bare minimum demands to enable joint incident handling. Next, teams can set a time schedule for developing to the *advanced* stage, for instance 1-2 years after achieving the basic stage. The *intermediate* stage offers some guidance for setting a growth path from basic towards advanced, although – depending on specific needs – some teams may opt to develop right from basic to advanced. The higher stages are in place to show that a national team has reached a higher level of maturity and that the conditions are met that enable interaction with CSIRTs worldwide reactively as well as pro-actively. It will also facilitate the building of trust between teams. Below a short explanation of the three stages is provided. For a more elaborate reasoning behind the minimum requirements for each level see the ENISA staged maturity model [6].

- ***Basic*** stage: for national CSIRTs to function adequately within their country and to work together with other teams (not just nationally but also globally or within their multinational economic region) they need to have a basic degree of maturity. Therefore, teams already must have a good foundation in regard to mandate, constituency, authority (etc.) – they need to be reachable and have a functional incident handling process. The values for the SIM3 parameters have been set in this manner for the *basic* stage: most organisational parameters will already need to score a fairly high level of maturity of at least 3, while most of the other parameters need to score only 1 or 2.
- ***Intermediate*** stage: this stage builds on the basic stage and especially aims at enabling higher management or legislative controls (level 4) for most of the organisational parameters, which were documented and approved (level 3) at the basic stage, without such controls. In the other areas (human, tools and processes) there is also gradual progress on most parameters.

- ***Advanced*** stage: for national CSIRTs to progress from merely 'working together' on handling incidents, to establishing a comprehensive coordinated incident management capacity - including effectively and reliably sharing threats, vulnerabilities and early-warning data with 'peer' national CSIRTs[4], it is essential that these teams reach a high level of maturity. The parameter values for the *advanced* stage have been set in this way. It means that most organisational parameters must score at level 4, whereas the human, tools and processes parameters must score at least 3, and in important cases even level 4.

The minimal required scores for the three maturity stages are specified in Table 4. As mentioned, Appendix A provides a more elaborate explanation of the relevance of each of the parameters for national CSIRTs, which also provides a further explanation of the minimum values for the different maturity stages.

Table 4 - Overview of ENISA maturity stages with minimal SIM3 score for each parameter

Parameter number	Parameter description	Minimum values for the stages:		
		Basic	Intermediate	Advanced
O-1	Mandate	3	4	4
O-2	Constituency	3	4	4
O-3	Authority	3	4	4
O-4	Responsibility	3	4	4
O-5	Service Description	3	4	4
O-7	Service Level Description	3	3	3
O-8	Incident Classification	1	2	3
O-9	Integration in existing CSIRT Systems	3	4	4
O-10	Organisational Framework	3	3	3
O-11	Security Policy	1	2	3
H-1	Code of Conduct/Practice/Ethics	2	3	3
H-2	Personnel Resilience	2	3	3
H-3	Skillset Description	1	2	3
H-4	Internal Training	1	2	3
H-5	External Technical Training	1	2	3

[4] Every CSIRT has 'peers' (fellow teams) that they work with closely and have a built trust to exchange potentially sensitive information.

H-6	(External) Communication Training	1	2	3
H-7	External Networking	2	3	3
T-1	IT Resources List	1	1	1
T-2	Information Sources List	1	2	3
T-3	Consolidated E-Mail System	1	2	3
T-4	Incident Tracking System	1	2	3
T-5	Resilient Phone	1	2	3
T-6	Resilient E-Mail	1	2	3
T-7	Resilient Internet Access	1	2	3
T-8	Incident Prevention Toolset	1	1	1
T-9	Incident Detection Toolset	1	1	1
T-10	Incident Resolution Toolset	1	1	2
P-1	Escalation to Governance Level	3	3	3
P-2	Escalation to Press Function	1	2	3
P-3	Escalation to Legal Function	1	2	3
P-4	Incident Prevention Process	1	2	2
P-5	Incident Detection Process	1	2	2
P-6	Incident Resolution Process	1	2	2
P-7	Specific Incident Processes	1	2	3
P-8	Audit/Feedback Process	2	3	4
P-9	Emergency Reachability Process	2	3	3
P-10	Best Practice E-mail and Web Presence	2	2	2
P-11	Secure Information Handling Process	2	3	3
P-12	Information Sources Process	1	2	3
P-13	Outreach Process	1	2	3
P-14	Reporting Process	2	3	4
P-15	Statistics Process	1	2	3
P-16	Meeting Process	1	1	2
P-17	Peer-to-Peer Process	1	1	2

How to use the Global CSIRT Maturity Framework

The Maturity Framework provides support and guidance to all national CSIRTs across the globe, including nations that are yet to establish a national CSIRT. In this chapter, different uses of the Maturity Framework are described. Throughout the chapter other relevant resources are mentioned that can contribute to the establishment and maturity of national CSIRTs. The information provided is meant as a supporting guideline for teams. It does not offer (prescriptive) predefined grow paths or cost estimates because this will vary strongly across contexts and is dependent on the specific ambition that a national CSIRT sets for itself.

For instance, in a country that already has several CSIRT activities running (e.g. for the government, and for the research & education community) it can be considerably easier and less costly to create a national CSIRT than in a country that has no such institutions yet. But also it makes a big difference in terms of time and money if the constituency of the national team is limited to the critical infrastructure sectors, or when it also includes e.g. all companies and citizens.

Establishing a national CSIRT

Depending on the specific context, parties involved in the process of establishing a (national) CSIRT may use this CSIRT Maturity Framework and the supporting CSIRT Maturity Kit [10] to navigate the vast range of possibilities and choices to be made when setting up a CSIRT. It is important to think about the underlying motivation for establishing a CSIRT, the institutional embedding, the governance structure, the mandate it may have, the target constituency, the services it will provide, etc.

Not a 'one-size-fits-all'

National CSIRTs are active in many nations around the world. There are differences in for example their mandate, size, governance structure and constituency. There is not one best way for setting up a national CSIRT. Depending on the context, different emphasis or choices are appropriate.

The 44 parameters as well as the maturity stage requirements can trigger parties to think about specific choices and options and help to establish a strategy and timeframe (roadmap) to achieve the aspired stage.

For instance, several parameters deal with the need for (trans)national cooperation – a need that is crucial for national CSIRTs, and reflected in the maturity stage values for these parameters. Therefore, it may be useful to explore the CSIRT landscape and identify relevant peer teams with whom future collaboration is expected or necessary. What kind of CSIRTs are operating within the country? Public or private? What services do they provide and

what is their constituency? Are there any other national CSIRTs with whom collaboration is foreseen? Working visits to exchange good practices and learn from other teams' efforts and experience are deemed extremely valuable.

During the development or enhancement of a national CSIRT, it is important to identify CSIRT services that need to be established as part of the national CSIRT initiative. The FIRST CSIRT Services Framework [7] provides a comprehensive list and description of the services a CSIRT can offer. As such, it allows an in-depth elaboration of what is referred to by the SIM3 parameters "service description" (O-5), and "service level description" (O-7).

The services are divided in 5 Service Areas, each containing several services and underlying functions. The Service Areas are:

1. Information Security Event Management
2. Information Security Incident Management
3. Threat Intelligence Management
4. Vulnerability Management
5. Knowledge Transfer

The FIRST CSIRT Services Framework is intended to support teams to choose their service portfolio. Not all teams will provide all services listed but typically a selection thereof, depending on their specific strategy and focus.

CSIRT maturity assessment

The Global CSIRT Maturity Framework makes it possible to assess the maturity of a (national) CSIRT. Assessment can be useful for setting a baseline score for internal review purposes. It can also be used as the starting point for maturity enhancement. Based on the baseline score, an action plan (including timeline) may be defined to improve to a next stage of maturity. Assessments can also be

Using a peer review approach

National CSIRTs can ask another team to perform a peer review of their self-assessment. A way to implement this is to ask a peer team to make available one of their more (experienced) staff members, who ideally has knowledge and experience with CSIRT maturity assessment. After the team has performed their self-assessment, the peer reviewer can go and meet them (experience teaches that such a meeting is most effective when done on-site) and discuss their results. This is in fact a win-win situation where both sides can learn from each other. It will help the team to make their self-assessment more accurate and show ways how to effectively increase maturity. It also contributes to a level of trust between the teams for future collaboration.

Note: all EU CSIRTs Network members use a combination of self-assessment and peer reviews to improve their maturity [6].

used to compare with peer CSIRTs using the Maturity Framework as guideline. Online self-assessment tools are available for SIM3[5].

The maturity stages defined in the Global CSIRT Maturity Framework are set as a good practice, to provide guidance for national CSIRTs. Some parameters may be of lesser relevance to a specific team whilst others are at the core of their strategy.

The CSIRT Maturity Framework may also be used to audit the maturity level of a (national) CSIRT to provide a certification or as proof of meeting specific requirements (for instance to be eligible for certain forms of support or collaboration). There are many ways of using a maturity model for requirement purposes, for example national CSIRT communities might prescribe the *basic* or *intermediate* maturity stage as the lowest common denominator and boundary for membership requirement of the given community.

CSIRT Maturity as requirement

- The European community of teams, TF-CSIRT (300+ members), was the first to use SIM3 as a requirement back in 2009, when they adopted SIM3 to define the highest level of their membership structure: 'Certified' [13].
- The NCA in Japan (over 300 CSIRT members) uses SIM3 since 2015 to improve the maturity of their member teams [8].
- The Global Forum on Cyber Expertise (GFCE) endorsed the CSIRT Maturity Kit in 2017, which uses SIM3 as backbone [10].
- The EU CSIRTs Network adopted the ENISA CSIRT maturity assessment methodology, which is based on SIM3, in 2018. It is used to assess and advance the capabilities of the EU CSIRTs Network members [6].
- The worldwide Forum of Incident Response and Security Teams (FIRST) is working on adopting (parts of) SIM3 for their membership process [9].

The parameters and maturity stages in the CSIRT Maturity Framework provide insight into the level of maturity of a national CSIRT. Additionally, the CERT/CC published an Incident Management Capability Assessment (IMCA) [14] that can be used to evaluate incident management and related capabilities to ensure that the right preparations and components are in place. The assessment evaluates if an organisation has the required components needed to formalise and sustain incident management capabilities, including the capabilities to detect incidents and maintain situational awareness, analyse incidents, and develop response and mitigations and proactively search for incidents and prevent them from (re)occurring.

[5] Two (online) measurement tools exist. The OCF tool aims at all sorts of CSIRTs worldwide [11]. ENISA's tool aims at national CSIRTs [12]. The OCF tool includes all properties of the ENISA tool, and provides more elaborate descriptions.

Concluding remarks

The global CSIRT Maturity Framework is meant to support the development and enhancement of national CSIRT capacities across the globe. Both established teams and countries that are still at the initiating phase of setting up a national CSIRT can use this framework to develop a roadmap to reach their specific ambitions. The framework offers guidance based on extensive experience from the CSIRT community, reflected in the use of well-established maturity models. However, it is not prescriptive and the maturity stages are meant as an inspiration and guideline. Due to specific (legal, institutional or cultural) circumstances in any given context it may be necessary to make different choices on several aspects. What the framework offers in any case is a common baseline and language to exchange practices and experiences across national CSIRTs all over the world.

References

1. Pawlak, P. & Barmpaliou, B.N. (2017) *Politics of cybersecurity capacity building: conundrum and opportunity*, Journal of Cyber Policy, 2:1, 123-144, DOI: 10.1080/23738871.2017.1294610
2. Global Good Practices - National Computer Security Incident Response Teams (CSIRTs): see https://cybilportal.org/publications/global-good-practices-national-computer-security-incident-response-teams-csirts/
3. Internet Worm, see https://spaf.cerias.purdue.edu/tech-reps/823.pdf
4. NatCSIRT: a worldwide grouping of recognised national CSIRTs, maintained by CERT/CC. For the NatCSIRT homepage see https://resources.sei.cmu.edu/news-events/events/natcsirt/, for their list of national teams see https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/
5. SIM3 model: https://opencsirt.org/maturity/sim3/
6. For 15 years, ENISA has been supporting EU Member States and CSIRT communities in Europe (https://www.enisa.europa.eu/csirts-map) to build and advance their incident response capabilities and capacities by providing good practice guidelines, online & onsite trainings and with dedicated CSIRT community projects. Since the introduction of the NIS Directive in 2016, ENISA has focused on the newly established network of dedicated CSIRTs (https://csirtsnetwork.eu/) and has developed their CSIRT three-tier maturity approach as well as their CSIRT maturity assessment methodology, together aimed at EU national response teams. The goal is to foster and advance operational cooperation and cross-border information exchange for stronger incident response in the EU.
   For the ENISA CSIRT three-tier maturity approach, see “ENISA CSIRT maturity assessment model” (https://www.enisa.europa.eu/publications/study-on-csirt-maturity)
   For the ENISA CSIRT maturity assessment methodology, see the “ENISA Maturity Evaluation Methodology for CSIRTs” (https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process)

7. FIRST CSIRT Services Framework: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
8. Nippon CSIRT Association (NCA): http://www.nca.gr.jp/en/
9. Based on private communication with the FIRST Membership Committee
10. GFCE CSIRT Maturity Kit: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/csirt-maturity-kit/CSIRT_MK_guide.pdf
11. The OCF SIM3 self-assessment tool is designed for worldwide use, and for all sorts of CSIRTs including national ones: https://sim3-check.opencsirt.org/
12. The ENISA SIM3 self-assessment tool includes the three-tier maturity approach, and is therefore mostly suited for use by national CSIRTs – bearing in mind that where ENISA uses the term “Certifiable” for the highest maturity stage, this is called “Advanced” in this document: https://www.enisa.europa.eu/csirts-maturity-sas
13. TF-CSIRT / Trusted Introducer use SIM3 as basis for the highest tier of their membership, the ‘Certified’ status: https://www.trusted-introducer.org/processes/certification.html
14. CERT/CC Incident Management Capabilities Assessment (IMCA): https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848

Appendix A – Annotated SIM3 description for nCSIRTs

Reprint[6] of the most relevant parts of the current version of SIM3, version mkXVIIIc (30 March 2015, c version 1 May 2019) – see https://opencsirt.org/maturity/sim3/ for the latest version.

The version below is annotated with an explanation of the three tier maturity stages for national CSIRTs. For each parameter, an explanation of relevance for nCSIRTs and the reasoning behind the required levels (0-4) per maturity stage (Basic, Intermediate and Advanced) is provided[7].

SIM3: Security Incident Management Maturity Model

Basic SIM3

The maturity model is built on three basic elements:

1) Maturity Parameters
2) Maturity Quadrants
3) Maturity Levels

The parameters are the quantities that are measured in regard maturity – over 40 exist and they are detailed below. Each Parameter belongs to one of four Quadrants. The Quadrants are therefore the main four categories of Parameters:

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

These four Quadrants have been chosen in such a way that the parameters in there are as mutually independent as possible.

[6] This reprint was authorised by the Open CSIRT Foundation, as were the "cuts" from the original, as well as the added explanations of the GCMF 2.0 version.

[7] The explanations are based on workshops with Andrea Dufkova, ENISA; Prof.Dr. Klaus-Peter Kossakowski, Hamburg University of Applied Sciences (HAW); Mirosław Maj, Open CSIRT Foundation (OCF); Don Stikvoort MSc, m7. These four defined the original three ENISA maturity tiers used for the GCMF. Dufkova represents ENISA, Maj the Open CSIRT Foundation that shepherds SIM3, and Stikvoort is the original author of SIM3. All four have 20+ years of international CSIRT experience. The conversations were facilitated and processed by TNO: Hanneke Duijnhoven, Bram Poppink, Tom van Schie.

What we really measure are the Levels for each Parameter. A desirable simplicity of the SIM3 has been reached by specifying a unique set of Levels, valid for all of the Parameters in all of the Quadrants:

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, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)

To make these five Levels even clearer, let’s have a look at what needs to be added to go from one level to the next:

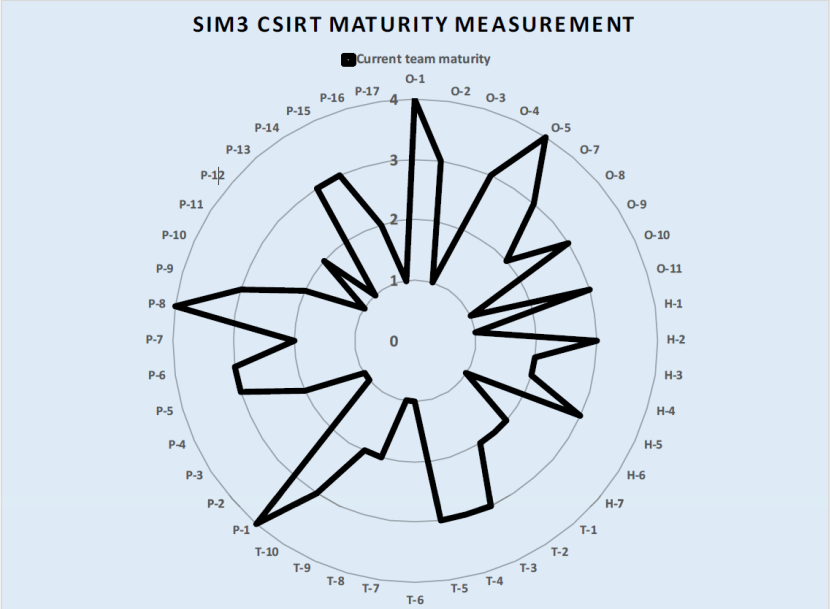
0 ➔ 1 : addition of *consideration* - “listen, we are aware of this”
1 ➔ 2 : addition of *written description* - “read, this is the way we do it”
2 ➔ 3 : addition of *accountability* - “look, this is what we are bound to do”
3 ➔ 4 : addition of *control mechanism* – “and this is how we make sure that it happens”

Such simplicity is great in terms of ease of use and presentation – but has its drawbacks too. This is especially noticeable in a few Parameters that, when you apply them in real life, are reluctant to be mapped onto a specific Level. However the advantages of this simplified scheme far outweigh the few quirks encountered.

SIM3 Reporting

The basic and most useful way to report a SIM3 assessment of an actual CSIRT has two elements:

1) A list of all the Parameters for the four Quadrants, with their respective assessed Levels – plus comments where due.
2) A “radar” diagram of all the Parameters and their assessed Levels.
{Example from the GCMF inserted to avoid confusion.}



SIM3 Parameters

The Maturity Parameters come with the following tags:

> [Parameter Identifier] : [Parameter Name:]
>
> Description:
>
> { OPTIONAL: Clarification: }
>
> { OPTIONAL: Minimum Requirement: }

This is mostly self-explanatory, with the exception of “minimum requirement” – now this field will be empty in many cases, but sometimes it is not sufficient for a Parameter to be only defined: the definition must also achieve some minimum level to be acceptable to the professional CSIRT community. An example is O-7, which is about "service level description" where the minimum level requires a human response within a certain number of working days. This way, the "minimum requirement" could help avoid empty placeholders, as clearly e.g. a defined and approved policy (Level 3) which states that reactions will be within one month, is useless and immature in the context of CSIRT operations.

The full list of Parameters is provided below.

O – “Organisation” Parameters

The organisational ('O') parameters focus on aspects that together describe the extend of the CSIRT’s activities (i.e. the mandate, setup *and services of the CSIRT, and the framework*

connecting all organisational aspects). National CSIRTS, by virtue of their national responsibility, should always be mandated by the government or through legislation to legitimately fulfil their national role. This also reflects on many of the other aspects related to the scope of their activities. For this reason, even at the Basic stage nCSIRTs should obtain relatively high levels of maturity on many of the O-parameters.

O-1 : MANDATE

Description: The CSIRT's assignment as derived from upper management.

GCMF Annotation:

O-1	Basic: 3	Intermediate: 4	Advanced: 4

For national CSIRTs, due to their national responsibility, the mandate comes from the government (a minister, regulator or other governmental body) or is derived from legislation. Without that mandate, the nCSIRT cannot function as a CSIRT with national responsibility. As a consequence, the maturity level of nCSIRTs on this parameter needs to move towards 4, and can effectively not be less than 3 at the Basic stage. When the mandate is formally and unambiguously derived from the government or legislation, this automatically means that the nCSIRT's management should have approved and formalised it internally because the mandate already has a formal status.

It follows from the above that the Intermediate and Advanced stage both require a level 4, which means that the nCSIRT's mandate is regularly controlled and/or reviewed in a formal process between the team and a higher governance level.

O-2 : CONSTITUENCY

Description: Who the CSIRT functions are aimed at – the "clients" of the CSIRT.

GCMF Annotation:

O-2	Basic: 3	Intermediate: 4	Advanced: 4

National CSIRTs have a national responsibility and it should therefore be clear how they fulfil this national role and who they provide services to (this can be the whole nation or specific target groups such as critical infrastructures, government organisations, etc.). This means that the constituency of an nCSIRT should be approved and/or defined by the government (it may even be written down in legislation). As a consequence, the maturity level of nCSIRTs on this parameter needs to move towards 4, and can effectively not be less than 3 at the Basic stage.

When the constituency is formally and unambiguously defined by the government or legislation, this automatically means that the nCSIRT's management should have approved and formalised it internally because the constituency already has a formal status.

It follows from the above that the Intermediate and Advanced stage both require a level 4, which means that the nCSIRT's constituency is regularly controlled and/or reviewed in a formal process between the team and a higher governance level.

O-3 : AUTHORITY

Description: What the CSIRT is allowed to do towards their constituency in order to accomplish their role.

GCMF Annotation:

O-3	Basic: 3	Intermediate: 4	Advanced: 4

Due to the fact that national CSIRTs are formally mandated by the government to fulfil a national role, the scope of their activities as reflected in the authority of the nCSIRT towards their constituency also needs to be approved by the government. As a consequence, the maturity level of nCSIRTs on this parameter needs to move towards 4, and can effectively not be less than 3 at the Basic stage. When it is formally and unambiguously defined by the government or legislation what the nCSIRT is allowed to do towards their constituency, this automatically means that the nCSIRT's management should have approved and formalised it internally because the authority of the nCSIRT already has a formal status.

It follows from the above that the Intermediate and Advanced stage both require a level 4, which means that the nCSIRT's authority is regularly controlled and/or reviewed in a formal process between the team and a higher governance level.

O-4 : RESPONSIBILITY

Description: What the CSIRT is expected to do towards their constituency in order to accomplish their role.

GCMF Annotation:

O-4	Basic: 3	Intermediate: 4	Advanced: 4

Due to the fact that national CSIRTs are formally mandated by the government to fulfil a national role, the scope of their activities as reflected in the responsibility of the nCSIRT

towards their constituency also needs to be approved by the government. As a consequence, the maturity level of nCSIRTs on this parameter needs to move towards 4, and can effectively not be less than 3 at the Basic stage. When it is formally and unambiguously defined by the government or legislation what the nCSIRT is expected to do towards their constituency, this automatically means that the nCSIRT's management should have approved and formalised it internally because the responsibility of the nCSIRT already has a formal status.

It follows from the above that the Intermediate and Advanced stage both require a level 4, which means that the nCSIRT's responsibility is regularly controlled and/or reviewed in a formal process between the team and a higher governance level.

O-5 : SERVICE DESCRIPTION

Description: Describes what the CSIRT service is and how to reach it.
Minimum requirement: Contains the CSIRT contact information, service windows, concise description of the CSIRT services offered and the CSIRT's policy on information handling and disclosure.

GCMF Annotation:

O-5	Basic: 3	Intermediate: 4	Advanced: 4

The service description of a CSIRT provides an overview of what services the team offers and how they offer them to their constituency. RFC2350 is commonly used as a standardised way to publish a high-level list of the team's services, contact info and service windows. The selection of services to offer should be based on the mandate, authority and responsibility of the team. For nCSIRTs, services may include incident management/response, awareness raising, information sharing and other services. The FIRST CSIRT Services Framework[8] provides a structured overview of service areas and specific services from which services are recommended to be selected. In case the services provided are named differently, it would be prudent to make a mapping between the services provided and the naming scheme of the FIRST CSIRT Services Framework.

For national CSIRTs, the scope of their activities is defined by the government (parameters O-1 to O-4). To make sure the activities of the nCSIRT are in line with its mandate as the national CSIRT, it is important that there is a clear and formalised description of the services that is approved by the nCSIRT's management. For nCSIRTs at the Basic stage, this can still be an

[8] See https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

internal team matter where the nCSIRT's management takes the responsibility to ensure that the services fit with the nCSIRT's mandate, authority and responsibility towards its constituents. However, for more mature teams (at the Intermediate and Advanced stage) it is important to regularly review the service description in a formal process between the team and a higher governance level to make sure the nCSIRT is still meeting the ambitions of the government with regard to cyber incident management and to support further improvements, as when both the team and the higher level are aware of the need and business case for specific service additions and improvements, it will pave the way to realise those.

O-6 : (intentionally left blank – not included in "scoring")

O-7 : SERVICE LEVEL DESCRIPTION

Description: Describes the level of service to be expected from the CSIRT.
Minimum requirement: Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CSIRTs. For the latter a human reaction within two working days is the minimum expected.

GCMF Annotation:

O-7	Basic: 3	Intermediate: 3	Advanced: 3

The CSIRT's service level description provides an overview of the service level the team commits to deliver for each service they offer. It describes what the constituents may expect from the team in terms of response time to incident reports or how often the team will provide advisories.

As with the selection of services, the service levels should align with the team's mandate, authority and responsibility. For national CSIRTs this means that the formal mandate as national CSIRT comes with certain authority and responsibility towards its constituents. The services provided, as well as the service levels should reflect the nCSIRTs mandate and the government ambitions and this should be formalised and written down. This means that the minimum level for this parameter for nCSIRTs is 3. At the same time, 3 is also the highest required level for all three maturity stages. There is no need for a higher authority to control or review the service level description because the mandate does not usually dictate a specific service level (for instance response times) nor is there an absolute 'right' service level to be offered. But if the mandate would include such SLAs, this would also need to be controlled. The translation of the mandate in service levels is about how the team assesses their own performance delivery in relation to the mandate.

O-8 : INCIDENT CLASSIFICATION

Description: The availability and application of an incident classification scheme to recorded incidents. Incident classifications usually contain at least “types” of incidents or incident categories. However, they may also include the “severity” of incidents.

GCMF Annotation:

O-8	Basic: 1	Intermediate: 2	Advanced: 3

For nCSIRTs, like any other CSIRT, it is important to work towards a good classification scheme for incidents. This will help not only in reporting statistics about the type of incidents that occur in the country and thus raising more awareness for this, but can also facilitate the prioritisation of handling incidents based on type and/or severity. Depending on the services and service levels of the nCSIRT, being able to report back on the incidents in annual reports or advisories can be important.

Until now, the incident response community has not developed a consistent classification scheme for national CSIRTs. For nCSIRTs at the Basic stage, it is acceptable to not have a fully developed classification method just as long as the nCSIRT members are able to keep track of different types of incidents. As the team matures, it is important to start developing a common structure or method to classify incidents. At the Intermediate stage, nCSIRTs should have an incident typology to work with amongst the team members. It is recommended to make use of an existing classification scheme (e.g. the Reference Security Incident Taxonomy, RSIT). To reach the Advanced level, the nCSIRT should have an incident classification scheme that is approved by the management of the team. The scheme should at least contain an incident typology, but it is also recommended to start including an impact or severity classification.

For some national teams, legislation may define specific incidents being part of their mandate. In such cases the legally defined incidents must be integrated into the incident classification used.

O-9 : INTEGRATION IN EXISTING CSIRT SYSTEMS

Description: Describes the CSIRT's level of membership of a well-established CSIRT co-operation, either directly or through an "upstream" CSIRT of which it is a customer/client. This is necessary to participate and integrate in the trans-national/worldwide CSIRT system(s).

GCMF Annotation:

O-9	Basic: 3	Intermediate: 4	Advanced: 4

It is useful to first note that an nCSIRT will rarely, if ever, have an "upstream" CSIRT: it is of paramount importance that nCSIRTs can freely roam and communicate inside the national, regional and global CSIRT communities.

In order to fulfil their national responsibilities, nCSIRTs have to be able to cooperate with other CSIRTs both nationally and internationally, including nCSIRTs from other countries or business sectors. Incidents often have a transnational character for which a joint collaborative response might be required. Because CSIRTs don't operate in a vacuum, they need to work together, share information and get to know each other to a certain extent. nCSIRTs represent a country, and therefore have to be visible and present in well-established CSIRT collaboration platforms and networks, such as FIRST. This means that nCSIRTs need to have a clear strategy on how they interact within the community and for what collaborations they will pursue membership.

The required level of 3 for the Basic stage reflects the importance for national teams to be present in national, regional and global networks – and this presence should be consistent, not dependent on the preferences of one or another team member involved in such cooperations. The description of the nCSIRTs level of membership and participation in CSIRT collaborations needs to be formalised and approved by the nCSIRT's management.

For the Intermediate and Advanced stages, the team needs to reach a level 4, which means that there is a control mechanism in place that audits the nCSIRT's integration in existing CSIRT networks systems. This is important as this parameter is one of the key success factors of any nCSIRT, because without proper integration into the CSIRT landscape worldwide, the nCSIRT will not get the information and timely reports that they need in order to fulfil their mandate. But also, the way that the nCSIRT performs this directly influences the reputation not only of the nCSIRT but also of the country in this global community. Therefore, it is imperative that the higher levels of governance audit this parameter, and discuss this with the team.

O-10 : ORGANISATIONAL FRAMEWORK

Description: Fits O-1 to O-9 together in a coherent framework document serving as the controlling document for the CSIRT.
Minimum requirement: Describes the CSIRT's mission and parameters O-1 to O-9.

GCMF Annotation:

O-10	Basic: 3	Intermediate: 3	Advanced: 3

The organisational framework is what is sometimes also called a 'team charter'. It is a coherent document that fits together the organisational setup of the CSIRT. It is for internal use and describes the team's mission, constitution of the team, who the team works for, what the team does and how this is mandated. The charter should include at least the parameters O-1 to O-9 and potentially a few more.

For nCSIRT, just as for any CSIRT, this is a very important document since it brings together all the elements that define and scope the work of the team. It reflects the internal policy of the nCSIRT and should therefore be validated and formalised by the nCSIRT's management. It reflects the formal government issued mandate of the nCSIRT and relates this to how the team performs its duties. Since the separate elements are already authorised and controlled by the necessary governance level, there is no need for this document to be subject to a control process with the higher governance level. This means that for nCSIRTs the required maturity level for all stages is 3.

O-11 : SECURITY POLICY

Description: Describes the security framework within which the CSIRT operates. This can be part of a bigger framework, or the CSIRT can have their own security policy.

GCMF Annotation:

O-11	Basic: 1	Intermediate: 2	Advanced: 3

If the nCSIRT is embedded in a host organisation (such as a Ministry or other public organisation), the host organisation will likely have IT or information security policies that will apply to the nCSIRT as well. If not, the team will need to have their own security policy. Most teams will aim for a security certification like ISO:27000.

For nCSIRTs it is recommended to gradually develop their security policy. Depending on the services and size of the nCSIRT, for many nCSIRTs at the beginning the security policy does not need to be very Advanced. It is more about having a lock on the door, a shredder, and basic hygiene more than technical implications. As the team grows and it takes up more Advanced services and activities the security policy will also need to be further developed.

At the Basic stage, it is required that the nCSIRT members are aware of security requirements related to their work but it is not yet required to have a formal, written security policy. As the team matures, the team will be able to gradually develop a well-thought through security policy that fits with their workflows and activities. At the Intermediate stage this should be

written down and known by all team members and as the team further matures it should become a formally adopted policy that is approved by the nCSIRT's management (Advanced stage).

H – "Human" Parameters

The human ('H') parameters in the framework focus on important aspects related to the CSIRT staff (this is not only about technical staff, but for staff members). Together, these parameters reflect how the team views its staff in relation to the work of the team and how this is organised. The aspects addressed by the parameters in this section are usually part of the internal management processes of the team and do not necessarily require regular control from governance levels above the CSIRT management. This means that for the three maturity stages for nCSIRTs, none of these parameters require a level higher than 3. Of course it is conceivable that in some countries, there will be a conceived need to have auditing and feedback from a higher level of governance on for instance the availability of sufficient staff (parameter H-2) or to help ensure they are properly educated (parameters H-4 to H-6) – and that could be a reason for a level 4 for these parameters – but in general such a level is not required for the three maturity stages.

H-1 : CODE OF CONDUCT/PRACTICE/ETHICS

Description: A set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work.
Clarification: E.g. the TI CCoP[9]. Behaviour outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.

GCMF Annotation:

H-1	Basic: 2	Intermediate: 3	Advanced: 3

Having a clear set of rules or guidelines for staff members on how to behave professionally and in an ethical manner is important for any CSIRT and is something that all staff members should be conscious off. Often these guidelines or sets of rules are written down in a Code of Conduct, Code of Practice and/or Code of Ethics. For nCSIRTs, the recommended minimum level at the Basic stage is 2. Due to the special mandate of an nCSIRT it is not enough to talk about how to behave and what is expected from staff members. The expectations of how the

[9] See https://www.trusted-introducer.org/TI-CCoP.pdf

staff behaves in specific situations should at least be written down and known by all staff members. From there, as a team becomes more mature (Intermediate and Advanced stages), the set of rules and guidelines should become formalised (level 3) at the level of the team (a document approved by the head of the team).

As many nCSIRTs are embedded in a government organisation, prevailing generic codes of conduct for civil servants or related guidelines may apply to nCSIRT staff members as well. Nevertheless, the nature of the work of an nCSIRT warrants specific sets of guidelines for the nCSIRT staff. For instance, about confidentiality, handling sensitive data, communication with different audiences and even how to behave privately with regard to computer security and cyber hygiene. The outward focus of an nCSIRT – as a mandated team with a national responsibility and focus – makes this even more important.

As alternative to the TI CCoP already mentioned, in 2020, the FIRST Special Interest Group on ethics published the 'Ethics for Incident Response and Security Teams' guideline[10]. This document discusses ethical aspects relevant to a code of conduct for CSIRTs.

H-2 : PERSONNEL RESILIENCE

Description: How CSIRT staffing is ensured during illness, holidays, people leaving, etc.
Minimum requirement: three (part-time or full-time) CSIRT members.

GCMF Annotation:

H-2	Basic: 2	Intermediate: 3	Advanced: 3

Personnel resilience means that there is enough staff available to deal with planned and unexpected absence of staff members and keep up the service levels that the team has committed to.

This parameter is closely related to the parameters that describe the team's services (parameter O-5) and service levels (parameter O-7), which in turn reflect the mandate (parameter O-1) of the team. If the service level states that the nCSIRT is operational 24/7, this automatically means that there should be enough staff members to fulfil this in a rotation. For nCSIRTs this is very important since they often have a very large and diverse constituency (with potentially a lot of requests for support). If there are no clearly set service levels or if there is a mismatch between service level and staffing, it will lead to problems for the staff

[10] https://ethicsfirst.org

members in responding to requests in a timely manner, which can lead to reputational damage.

This means that at the Basic stage there should be a written description of how the nCSIRT deals with staffing in relation to the service levels (addressing how much staff is needed to provide the appropriate service level, how the roster is organised and how is dealt with planned and unplanned absences). Since staffing is an aspect that is mostly dealt with internally within the team, the Intermediate and Advanced stages require a level 3, meaning that this is a formalised statement that is approved by the management of the team.

H-3 : SKILLSET DESCRIPTION

Description: Describes the skills needed on the CSIRT job(s).

GCMF Annotation:

H-3	Basic: 1	Intermediate: 2	Advanced: 3

Just as it is important to have a clear understanding of how many staff members are needed to be able to offer the nCSIRT's services portfolio and the corresponding service levels that the team is committed to, it is also important to know what skills each role in the team requires. It is important here to not only focus on technical skills but also on communication, project management and other relevant skills, as well as experience levels required. For nCSIRTs communication and stakeholder outreach skills are generally very important due to their specific position and mandate. Depending on the types of services (defined in parameters O-5 and O-7), other specific skills or knowledge profiles also need to be addresses.

For an nCSIRT at the Basic stage there should be an understanding among staff and especially team management of the skills needed for each role (in relation to the specific services). At the Intermediate stage, there needs to be a document that describes the skillsets. Since staffing is an aspect that is mostly dealt with internally within the team, the Advanced stage requires a level 3, meaning that this is a formalised skillset description that is approved by the management of the team.

As many nCSIRTs are be embedded in a government organisation, generic descriptions of skillsets for civil servants may be available, but these are not adequate here. The description should be specific for the nCSIRT staff and aligned with the services and mandate of the nCSIRT.

H-4 : INTERNAL TRAINING

Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones.

GCMF Annotation:

H-4	Basic: 1	Intermediate: 2	Advanced: 3

Continuous development of staff is important to keep the staff motivated and to ensure the necessary skills and competences to meet the required skillsets (H-3) are available and up-to-date. This parameter focuses on the policy of the nCSIRT with regard to internal training of new staff members (onboarding) and existing staff members to improve their skills.

An nCSIRT in the Advanced stage will have a formalised policy about internal training (approved by the nCSIRT management) that addresses how the training needs are identified, what trainings are available for which staff members, how they are provided (mentoring programme, training days, peer-to-peer guidance) and monitored. At the Basic stage, there should at least be an understanding how the process of internal training works, because with that, there is no way to get new team members up-to-speed. At the Intermediate stage team members need to have written down how this process works, and have something like a checklist with the necessary minimum of items that the new staff member needs to know, learn and do – and be engaged in. Such a checklist can be on the team wiki or similar team information facility, and does not need to formalised for the Intermediate stage.

Note that newer, less mature, teams will not be able to offer a very broad range of internal training and the catalogue will likely grow as the team matures and staff members gain more experience. This parameter, however, is not about how many trainings are offered or about the range of the training catalogue. It is about how the processes surrounding internal training of staff are organised and how thoroughly this is documented and formalised.

H-5 : EXTERNAL TECHNICAL TRAINING

Description: Program to allow staff to get job-technical training externally – like TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.)

GCMF Annotation:

H-5	Basic: 1	Intermediate: 2	Advanced: 3

Continuous development of staff is important to keep the staff motivated and to ensure the necessary skills and competences to meet the required skillsets (parameter H-3) are available and up-to-date. This parameter focuses on the policy of the nCSIRT on technical training for staff members, which is usually (but not always) taking place externally. All types of CSIRTs, including national teams, will need technical expertise in various areas. The differences between different CSIRTs lie partially in the kind of technical expertise needed to do their job well, and this depends on the team's mandate (parameter O-1), responsibility (parameter O-4) and services (parameter O-5). For instance, an nCSIRT will need to have more technical knowledge dealing big scale incidents, APTs, massive DDoS, spear phishing, intel attacks – and less focus on specific hardware/software like organisational CSIRTs might do.

At the Basic stage, there is not a training programme or policy but there are opportunities for staff members to enrol in external technical trainings when deemed necessary. Also, nCSIRT staff members are aware of these possibilities and know how to apply for them with the team's management. As the team matures, a training programme and process will be written down for the staff members to refer to (Intermediate stage) and finally (Advanced stage) the provision of external technical training to staff members will be formalised in a policy that is approved by the nCSIRT's management.

H-6 : (EXTERNAL) COMMUNICATION TRAINING

Description: Program to allow staff to get (human) communication/presentation training externally.

GCMF Annotation:

H-6	Basic: 1	Intermediate: 2	Advanced: 3

Together with technical expertise, communication skills are among the most important competences that CSIRT staff members should possess. This holds especially true for national CSIRTs due to their national responsibility and focus. Communicating with external audiences is a core element in all of the team's activities. This parameter reflects the team's policy on providing (often external) communication training to ensure that the staff members can meet with the required skillsets (parameter H-3) for the specific nCSIRT roles and services (as defined in parameter O-5).

At the Basic stage there does not have to be a written policy, but staff members should be aware of the importance of communication and know what the possibilities are to enhance their communication skills. As the nCSIRT matures, a communication training programme and

process should be written down for the staff members to refer to (Intermediate stage) and finally (Advanced stage) the provision of communication training to staff members will be formalised in a policy that is approved by the nCSIRT's management.

H-7 : EXTERNAL NETWORKING

Description: Going out and meeting other CSIRTs. Contributing to the CSIRT system when feasible.

GCMF Annotation:

H-7	Basic: 2	Intermediate: 3	Advanced: 3

Collaboration with other teams is one of the core pillars of the CSIRT community. Engaging with other CSIRTs should therefore be a part of the job description of all staff members. This parameter describes what the team does to stimulate and support external networking and is related to (a requirement for) parameters O-9, O-10, P-13, and P-17. Sending staff members to conferences or meetings is important to put the plans and processes described in these parameters to practice (for instance without it, listing that you are a member of an international collaboration is only a membership on paper and not a true collaboration).

For nCSIRTs in particular, due to their coordinating nature, engaging with other CSIRTs in the country and nCSIRT in other countries is an important success factor. Therefore, the Basic stage requires that there is a thought-out, written description of what is expected of staff members and how it is ensured that all staff members are involved in external networking (and not just the one, senior, staff member). For the Intermediate and Advance stages, this should be a formal policy that is approved by the nCSIRT's management.

T – "Tools" Parameters

T-1 : IT RESOURCES LIST

Description: Describes the hardware, software, etc. commonly used in the constituency, so that the CSIRT can provide targeted advice.

GCMF Annotation:

T-1	Basic: 1	Intermediate: 1	Advanced: 1

For a national CSIRT it is very difficult (or even impossible) to maintain a good and up-to-date list of the most important and commonly used IT resources in their constituency, since the

constituency of an nCSIRT is generally extremely diverse. Therefore, it is not expected to obtain higher than level 1 on this parameter for a national CSIRT, meaning that there is awareness amongst the team members about the types of IT resources the nCSIRT can offer support for to specific parts of the constituency (e.g. critical infrastructure related) and what IT resources are most critical.

For nCSIRTs, despite the relatively low maturity requirements, it is recommended to focus on developing an overview of IT resources that are most critical for the constituency, especially for instance for CII. From there, the nCSIRT can develop more advanced knowledge and provide detailed and targeted advice about these critical IT resources.

T-2 : INFORMATION SOURCES LIST

Description: Where does the CSIRT get their vulnerability/threat/scanning information from.

GCMF Annotation:

T-2	Basic: 1	Intermediate: 2	Advanced: 3

The information sources list is deemed to be very important for national CSIRTs because most nCSIRTs need to be able to pass relevant information to its constituency (although this depends on the services as defined in parameter O-5).

Regardless of the extent to which information sharing is a key service that an nCSIRT offers, the team should have a good overview of what sources they obtain their information from. National CSIRTs have a very narrow margin for mistakes, since the trustworthiness of the nCSIRT and even the government is at stake. Therefore, an nCSIRT should maintain a very good information sources list. In addition, national CSIRTs usually work with a broad range of information sources (including specific cybersecurity information sources and more 'general' sources such as social media, news items, parliamentary information) that vary in trustworthiness and quality or depth of information. To keep track of all these sources and the information coming from these sources nCSIRTs generally need to pay more attention to the information sources list, compared to other teams. It is recommended to use a tool for storing this information, including an explanation about how trustworthy a source is.

At the Basic stage, it may be acceptable to keep track of information sources without having a written list or tool to document the sources, especially if there are experts in the team who have a clear overview of the information sources in their head. As the team matures and grows, not having a written down list of information sources is no longer acceptable because there are most likely more people working with the sources and processing the information.

To work towards the Advanced stage nCSIRT should develop a process for approval of adding items to the information list, as well as a process for determining the trustworthiness of a source. At the Advanced stage the information sources list and particularly the procedures of working with the list should be written down and formally approved by the nCSIRT's management.

T-3 : CONSOLIDATED E-MAIL SYSTEM

Description: When all CSIRT mail is (at least) kept in one repository open to all CSIRT members, we speak of a consolidated e-mail system.

GCMF Annotation:

T-3	Basic: 1	Intermediate: 2	Advanced: 3

For nCSIRTs, just like other CSIRTs, it is important to ensure that all incident responders have access to the same set of information, including incoming emails addressed to the CSIRT. Usually, it is implemented as a ticketing system, such that incoming emails are stored as tickets in this system.

Even at the Basic stage all incident responders should have access to the right information. However, it is acceptable that the nCSIRT has not explicitly recognised and formally decided that there should be a consolidated email system to realise this. As the team matures, it should become a conscious decision to have a system that ensures access to emails for all the team members. The requirements and manual of the system should be written down and known by all team members (Intermediate stage). At the Advanced stage this should be formally approved, implemented and periodically revisited by the nCSIRT's management.

T-4 : INCIDENT TRACKING SYSTEM

Description: A trouble ticket system or workflow software used by the CSIRT to register incidents and track their workflow.
Clarification: RTIR, AIRT, OTRS, trouble ticket systems in general.

GCMF Annotation:

T-4	Basic: 1	Intermediate: 2	Advanced: 3

For nCSIRTs, just like other CSIRTs, it is important to ensure that all incident responders have access to the same set of information, especially when it comes to incident reports. Usually, it

is implemented as a ticketing system, such that incident reports are registered and stored as tickets in this system.

Even at the Basic stage all incident responders should have access to the right information. However, it is acceptable that the nCSIRT has not explicitly recognised and formally decided that there should be an incident tracking system to realise this. As the team matures, it should become a conscious decision to have a system that facilitates incident tracking and that is accessible for all the team members. The requirements and manual of the system should be written down and known by all team members (Intermediate stage). At the Advanced stage this should be formally approved, implemented and periodically revisited by the nCSIRT's management.

T-5 : RESILIENT PHONE

Description: The phone system available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.
Clarification: Mobile phones are the easiest fall-back mechanism for when a team's landlines are out of order.
Minimum requirement: Fall-back mechanism for the case of phone system outages

GCMF Annotation:

T-5	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs, just like other CSIRTs, should always have access to the phone system and its services in order for constituents and partners to reach the nCSIRT. This relates also to the service levels that the nCSIRT commits to (parameter O-7). The service level of the phone system - as obtained from the IT department of the organisation the nCSIRT is embedded in or another provider - should fit with the nCSIRTs service level description. For instance, if the nCSIRT promises to be available 24/7 for reporting incidents by phone, this means that the service level agreement with the phone system provider should be in accordance. If the provider cannot commit to that service level, the nCSIRT should revisit and adjust their own service levels or make sure that resilience is obtained in another way (mobile phones as backup system).

At the Basic stage, the phone system is working, it seems to be well organised, but the team has never consulted the provider the service level agreements of this system. The team is aware of the resilience of the phone service to a certain extent. If the team is not aware of the resilience at all, they have not yet reached the minimum required level 1. At the Intermediate

stage, the team is aware of how resilient the phone service is and this is documented within the team. At the Advanced stage the nCSIRT's management should agree on whether the resilience level is acceptable and aligned with the service level description of the team. In addition, nCSIRT management periodically reassesses the phone system and its resilience.

As national CSIRTs are quite visible, they are an attractive target for (state-sponsored) attacks, hence it is recommended to grow to the Intermediate/Advanced stages rather quickly.

NB: the awareness of resilience at the nCSIRT team is not the same as an actual high resilience of the service itself.

T-6 : RESILIENT E-MAIL

Description: The e-mail system available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.

GCMF Annotation:

T-6	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs, just like other CSIRTs, should always have access to the email system and its services in order to properly register emails from constituents and other partners and to respond in a timely manner. This relates also to the service levels that the nCSIRT commits to (parameter O-7). The service level of the email system - as obtained from the IT department of the organisation the nCSIRT is embedded in or another provider - should fit with the nCSIRTs service level description. For instance, if the nCSIRT promises to respond to emails within 24 hours, this means that the service level agreement with the email system provider should be in accordance (there cannot be an outage >24h). If the provider cannot commit to that service level, the nCSIRT should revisit and adjust their own service levels or make sure that resilience is obtained in another way (e.g. backup system).

At the Basic stage, the email system is working, it seems to be well organised, but the team has never consulted the provider the service level agreements of this system. The team is aware of the resilience of the email service to a certain extent. If the team is not aware of the resilience at all, they have not yet reached the minimum required level 1. At the Intermediate stage, the team is aware of how resilient the email system is and this is documented within the team. At the Advanced stage the nCSIRT's management should agree on whether the resilience level is acceptable and aligned with the service level description of the team. In addition, nCSIRT management periodically reassesses the email system and its resilience.

As national CSIRTs are quite visible, they are an attractive target for (state-sponsored) attacks, hence it is recommended to grow to the Intermediate/Advanced stages rather quickly.

NB: the awareness of resilience at the nCSIRT team is not the same as an actual high resilience of the service itself.

T-7 : RESILIENT INTERNET ACCESS

Description: The Internet access available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.

GCMF Annotation:

T-7	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs, just like other CSIRTs, should always have access to Internet and its services in order to perform their activities and deliver its services. This relates also to the service levels that the nCSIRT commits to (parameter O-7). The service level of the Internet - as obtained from the IT department of the organisation the nCSIRT is embedded in or another provider - should fit with the nCSIRTs service level description. For instance, if the nCSIRT promises to respond to incident reports within 24 hours, this means that the service level agreement with the Internet provider should be in accordance (there cannot be an outage >24h). If the provider cannot commit to that service level, the nCSIRT should revisit and adjust their own service levels or make sure that resilience is obtained in another way (e.g. backup internet access, such as 4G, ADSL).

At the Basic stage, the Internet access is working, it seems to be well organised, but the team has never consulted the provider the service level agreements of this system. The team is aware of the resilience of the Internet access to a certain extent. If the team is not aware of the resilience at all, they have not yet reached the minimum required level 1. At the Intermediate stage, the team is aware of how resilient the Internet access is and this is documented within the team. At the Advanced stage the nCSIRT's management should agree on whether the resilience level is acceptable and aligned with the service level description of the team. In addition, nCSIRT management periodically reassesses the Internet access and its resilience.

As national CSIRTs are quite visible, they are an attractive target for (state-sponsored) attacks, hence it is recommended to grow to the Intermediate/Advanced stages rather quickly.

NB: the awareness of resilience at the nCSIRT team is not the same as an actual high resilience of the service itself.

T-8 : INCIDENT PREVENTION TOOLSET

Description: A collection of tools aimed at preventing incidents from happening in the constituency. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: e.g. IPS, virus scanning, spam filters, port scanning. If not applicable as for a purely co-ordinating CSIRT, choose -1 as Level and will be omitted from "scoring".

GCMF Annotation:

T-8	Basic: 1	Intermediate: 1	Advanced: 1

For some national CSIRTs, an incident prevention toolset is not critical for fulfilling their mandate and responsibility. This toolset is related to the team's incident prevention process (parameter P-4). Some teams are consciously not involved in prevention, though when observed closely, this is actually rare. In those cases, the team can opt for a level -1 which means that the parameter is not relevant and is omitted in the assessment of the overall maturity level (Basic, Intermediate and Advanced stages).

If prevention is a service that the nCSIRT provides to its constituency, the team should at least be aware of what tools are used for this task.

Higher levels are not required for the Intermediate and the Advanced stage at this point in time, but when prevention is a conscious part of the services portfolio, it is recommended to consider going to levels 2 or even 3.

T-9 : INCIDENT DETECTION TOOLSET

Description: A collection of tools aimed at detecting incidents when they happen or are near happening. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: e.g. IDS, quarantinenets, netflow analysis.

GCMF Annotation:

T-9	Basic: 1	Intermediate: 1	Advanced: 1

This toolset is related to the team's incident detection process (parameter P-5). Every nCSIRT needs to have at least a basic detection toolset that that is used to detect and/or record what incidents are taking place in their constituency. It is relevant to note that the Consolidated Email System (parameter T-3) which is used to report incidents by the constituency to the nCSIRT is also an incident detection tool, as is the Incident Tracking System (parameter T-4). But often there are additional tools for detection, as in the examples mentioned above. Sometimes the same tool is used for both incident prevention and detection.

All nCSIRT members should at least be aware of what tools they use for incident detection.

Higher levels are not required for the Intermediate and the Advanced stage at this point in time, but it is recommended to consider going to levels 2 or even 3.

T-10 : INCIDENT RESOLUTION TOOLSET

Description: A collection of tools aimed at resolving incidents after they have happened. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: E.g. basic CSIRT tools including whois, traceroute etc; forensic toolkits.

GCMF Annotation:

T-10	Basic: 1	Intermediate: 1	Advanced: 2

Incident resolution is, generally speaking, the core task performed by any CSIRT, including nCSIRTs. As a consequence, all CSIRTS will have some type of tool for this, even if basic at first. This toolset is related to the team's incident resolution process (parameter P-6). It is relevant to note that the Consolidated Email System (parameter T-3) which is used to report incidents by the constituency to the nCSIRT is also an incident resolution tool, as is the Incident Tracking System (parameter T-4). But usually there are additional tools for resolution, as in the examples mentioned above. Sometimes the same tool is used for both incident detection and resolution.

At the Basic and Intermediate stage, the team should be aware of what tools are used for incident resolution. It is more urgent to have the incident resolution process (parameter P-6) in place, and less urgent to explicitly write down what tools you use.

However, it is very helpful to have a written description of the incident resolution toolset to ensure all team members are aware of this. This is also helpful when new people join the team, and need to know how incident resolution works, and what tools they should be able to use.

And therefore, at the Advanced stage level 2 is demanded. Higher levels are not required at this point in time, but it is recommended to consider going to level 3.

P – "Processes" Parameters

The process ('P') parameters focus on a set of processes that should be well organised in order for an nCSIRT to perform its tasks. The word "process" is meant in a generic way – it includes not only processes in the sense of a logical set of sequential/parallel steps, but also policies, both of the more fundamental kind as well as very basic policies. Some of the process parameters are connected with parameters from the other areas (Organisation, Human, and Tools), where the description or list is more in those other areas, and the P-parameters focus on the steps that need to be taken.

To give an example: T-2, the Information Sources List is connected with parameter P-12, the Information Sources Process. In T-2 all the sources where the CSIRT gets their information from should be listed, whereas P-12 then explains how to use those different sources.

P-1 : ESCALATION TO GOVERNANCE LEVEL

Description: Process of escalation to upper management for CSIRTs who are a part of the same host organisation as their constituency. For external constituencies: escalation to governance levels of constituents.

GCMF Annotation:

P-1	Basic: 3	Intermediate: 3	Advanced: 3

Escalation to governance level is a core process of an nCSIRT. It is necessary for any CSIRT to have a short and effective escalation path to higher levels of governance (including the highest level), which for nCSIRTs usually means the highest levels of government and related agencies. The reason for this is that when an incident is critical, it is obvious that those highest levels must be informed quickly, even outside office hours. The relevant minister(s) will need to be informed, maybe even the prime minister – and very quickly, the press will be on the phone, parliament will ask questions, and so on. An escalation chains with many steps will inevitably fail to achieve the goal of quick escalation. Therefore, a quick and short escalation path is a necessity. This usually requires shortcuts through the layers of the "chain of command", shortcuts that will also work late on Sunday evening, or at three in the night.

The three maturity stages all require a 3 because this exception process to escalate to higher government level in case of very serious incidents, needs to be approved and formalised at the

level of the nCSIRT management, and written down – or else it will never work in case of an emergency. It is necessary that there is some threshold to invoke this process, as it is at no one's interest when an individual team member decides on their own to warn the highest levels. Therefore, something like a four-eyes process, or involvement of the head of the team or their deputy, is recommended.

Even when this process may have been approved on the highest levels, that does not warrant level 4 for this parameter and as such, level 4 is not required. To obtain level 4, it would take an active form of auditing on the workings of this process – or it to be included in national law, as could for instance be the case when the escalation is part of a national crisis management system.

P-2 : ESCALATION TO PRESS FUNCTION

Description: Process of escalation to the CSIRT's host organisation's press office.

GCMF Annotation:

P-2	Basic: 1	Intermediate: 2	Advanced: 3

For nCSIRTs it is important to have influence over what information is shared with the press about ongoing (or past) security incidents, and when. The relationship with the press is often indirect, for example when the press relations are dealt with by a press office in the parent organisation. In general, only larger national teams have their own press spokespeople. But no matter where the press contacts are being handled, the team needs to know those spokespeople, and be able to reach them effectively and at all times – and vice versa. Without such an escalation process, the risk is too high that when a serious incident occurs, and the press will be asking questions, that the spokespeople will give uninformed answers which may lead to reputational or other types of damage – and even saying "we don't know" can lead to serious damage at critical moments in time.

At the Basic stage what the nCSIRT needs as a minimum is a working method to reach and inform the spokespeople, i.e. the press function – this does not have to be written down, as long as the team know how and when to use it. Grounding and documenting this process is clearly in the interest of both the nCSIRT and the press function, as that will make the outcome of the process more reliable, especially outside business hours. This means that all involved need to know when as escalation is due, how to do the escalation, and how to reach the press function. The spokespeople themselves need to know what to expect, and to be available for

such escalations. Therefore, a growth to the Intermediate stage with level 2 and the Advanced stage with level 3 is seen as necessary.

There is rarely an explicit need to obtain level 4 here, nor is it common that this process is mentioned in national law.

P-3 : ESCALATION TO LEGAL FUNCTION

Description: Process of escalation to the CSIRT's host organisation's legal office.

GCMF Annotation:

P-3	Basic: 1	Intermediate: 2	Advanced: 3

For nCSIRTs it is important to be able to consult with legal experts on matters where the action or inaction of the team might lead to legal issues (liability and other risks). Such legal experts usually reside in a legal function, or legal office, in the parent organisation. In general, only larger national teams have their own legal experts. But no matter where the legal function is situated, the team needs to know those legal experts, and be able to reach them effectively and at all times. Without such an escalation process, the risk is too high that when a serious incident occurs, it will take too much time to reach the legal function, plus those legal experts may then not be too aware of the specific situation and needs of the nCSIRT.

At the Basic stage what the nCSIRT needs as a minimum is a working method to escalate to the legal function – this does not have to be written down, as long as the team know how and when to use it. Grounding and documenting this process is clearly in the interest of both the nCSIRT and the legal function, as that will make the outcome of the process more reliable, especially outside business hours. This means that all involved need to know when as escalation is due, how to do the escalation, and how to reach the legal function. The legal experts themselves need to know what to expect, and to be available for such escalations. Therefore, a growth to the Intermediate stage with level 2 and the Advanced stage with level 3 is seen as necessary.

There is rarely an explicit need to obtain level 4 here, nor is it common that this process is mentioned in national law.

P-4 : INCIDENT PREVENTION PROCESS

Description: Describes how the CSIRT prevents incidents, including the use of the related toolset. Also, this includes the adoption of pro-active services like the issuing of threat/vulnerability/patch advisories.

GCMF Annotation:

P-4	Basic: 1	Intermediate: 2	Advanced: 2

The incident prevention process is about the procedural aspects of those nCSIRT services aimed at incident prevention, and describes step by step how the team provides such services to its constituency. Part of the prevention process can be services such as:

- *the creation and dissemination of advisories about new security vulnerabilities;*
- *port scan activities;*
- *the spreading of threat intelligence;*
- *the sharing of lessons learnt from the analysis of incidents.*

Usually, tools are used to support these processes (see parameter T-8).

In some cases, nCSIRTs do not engage themselves with incident prevention. In those cases, level -1 can be chosen (meaning: not applicable), and P-4 will then be omitted in the assessment of the overall maturity level (Basic, Intermediate and Advanced stages).

The required level 1 at the Basic stage shows that there is no need to immediately formalise or write down the incident prevention process from the start. The process should be known by the people that are tasked to perform it. However, it is problematic to discuss and train team members on a process that has not been written down. Therefore, level 2 is required for the Intermediate and Advanced stages. This is typically a process that is detailed, usually step-by-step with text and process diagrams, on a team wiki or similar team information sharing facility. It is certainly worthwhile to go beyond level 2, but this is (currently) not required for the Advanced stage.

P-5 : INCIDENT DETECTION PROCESS

Description: Describes how the CSIRT detects incidents, including the use of the related toolset.

GCMF Annotation:

P-5	Basic: 1	Intermediate: 2	Advanced: 2

The incident detection process is about the procedural aspects of those nCSIRT services aimed at incident detection, and describes step by step how the team provides such services to its constituency. Tools are used to support these processes (see parameter T-9). Some nCSIRTs

have their own detection tools, and these can be highly advanced or rather basic: tools for the receiving and initial assessment (called "triage") of incident reports coming in via e-mail, webforms and the telephone using the team's incident tracking system. nCSIRTs may also include as part of their detection process the handling of information from e.g. a SOC, or other partners.

Often, the incident detection process is combined with the incident resolution process (parameter P-6), as the steps from incident detection and reporting/monitoring to resolution form a logical whole, often referred to as the incident handling process.

The required level 1 at the Basic stage shows that there is no need to immediately formalise or write down the incident detection process from the start. The process should be known by the people that are tasked to perform it. However, it is problematic to discuss and train team members on a process that has not been written down. Therefore, level 2 is required for the Intermediate and Advanced stages. This is typically a process that is detailed, usually step-by-step with text and process diagrams, on a team wiki or similar team information sharing facility. It is certainly worthwhile to go beyond level 2, but this is (currently) not required for the Advanced stage.

P-6 : INCIDENT RESOLUTION PROCESS

Description: Describes how the CSIRT resolves incidents, including the use of the related toolset.

GCMF Annotation:

P-6	Basic: 1	Intermediate: 2	Advanced: 2

The incident resolution process is about the procedural aspects of those nCSIRT services aimed at incident resolution, and describes step by step how the team provides such services to its constituency. Tools are used to support these processes (see parameter T-10). Some nCSIRTs have their own detection tools. These can be both highly advanced or rather basic: tools including email and the incident tracking system, but also e.g. highly advanced forensics toolkits.

Every nCSIRT has an incidents resolution process and will have to develop at least a generic process about how to resolve, handle, mitigate incidents. Often, the resolution process is combined with the incident detection process (parameter P-5), as both form a logical whole.

The required level 1 at the Basic stage shows that there is no need to immediately formalise or write down the incident resolution process from the start. The process should be known by the people that are tasked to perform it. However, it is problematic to discuss and train team members on a process that has not been written down. Therefore, level 2 is required for the Intermediate and Advanced stages. This is typically a process that is detailed, usually step-by-step with text and process diagrams, on a team wiki or similar team information sharing facility. It is certainly worthwhile to go beyond level 2, but this is (currently) not required for the Advanced stage.

P-7 : SPECIFIC INCIDENT PROCESSES

Description: Describes how the CSIRT handles specific incident categories, like phishing or copyright issues.
Clarification: may be part of P-6.

GCMF Annotation:

P-7	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs deal with various sorts of incidents and teams need to work on those in a time and cost-effective way. This also means that over time, ways are found to more effectively handle specific types of incidents that occur frequently, or have greater impact. When such ways are written down into specific processes, as additions or alternatives to the generic process of P-6 above, we refer to them as "specific incident processes". These can be on any number of topics that are of special significance for the nCSIRT in question, ranging from technical incidents like massive DDoS attacks in the country, to reputational damage type of incidents. Often, these will also have higher priority (see O-8). Also, some incident category can be so highly automated, that it warrants a specific description.

Newly starting teams require level 1 for the Basic stage, meaning that specific incident processes are performed as a way of working, in line with the P-6 process. Teams will acquire experience along the way about what types of incidents are important to them and which incident types require more specific handling. And as it is problematic to discuss and train team members on a process that has not been written down, level 2 is required for the Intermediate stage. P-7 (like P-6) is typically a process that is detailed, usually step-by-step with text and process diagrams, on a team wiki or similar team information sharing facility.

Sometimes, P-7 is written down as an "exceptions" part of P-6. However, for P-7 the Advanced stage requires level 3, which is not currently required for P-6. This is because it is seen as crucial

that nCSIRTs at the Advanced stage have specific processes in place for critical and/or frequently occurring types of incidents. This improves efficiency and enables the nCSIRT to handle more incidents using fewer resources and time. And then management approval of such a process, bringing it to level 3, is deemed necessary.

P-8 : AUDIT/FEEDBACK PROCESS

Description: Describes how the CSIRT assesses their set-up and operations by self-assessment, external or internal assessment and a subsequent feedback mechanism. Those elements considered not up-to-standard by the CSIRT and their management are considered for future improvement.

GCMF Annotation:

P-8	Basic: 2	Intermediate: 3	Advanced: 4

The audit and feedback process is very important for an nCSIRT because this process affects all activities and aspects of an nCSIRT, including all other parameters. It can be seen as the process that is in place to perform quality assurance checks and to draw lessons from the results that relate to all activities performed by the nCSIRT. Therefore, it is also the process that warrants other parameters to potentially reach a level of 4 – with the exception of those cases where the national law already ensures that specific parameters can reach level 4.

Sometimes, aspects of the audit/feedback process are embedded in national law and therefore even legally mandatory for teams to implement. Oftentimes, the execution of this process falls into two categories: the first is what the team does internally in regards self-assessment and quality control, and the second is where an external auditing or feedback process takes place. In the case of nCSIRTs this is usually done by some kind of government auditing department.

Both categories are important and it is good to realise the caveats for both. For the self-assessments it is necessary to realise that those are very valuable and allow the team to internally learn and grow. However, an internal assessment process is not sufficient to allow any parameter to go higher than level 3, by definition, as this kind of assessment stays inside the team – and just sending a report about it to higher levels of governance does not count as level 4 yet.

If audits are done by an audit department and this is well anchored within the organisation, then this likely warrants a level 4 for the P-8 parameter itself, but not necessarily for any other parameter: for that to happen, it needs to be made more specific for the audit department

what to audit. Audit departments usually and understandably demand to be free in their choice and methodology, which means it is recommended to request them to audit at least a subset of aspects, corresponding with an explicit selection of the GCMF parameters that the team finds most critical for their functioning and where they seek the active involvement of the higher governance levels.

For the Basic stage level 2 is required, which means that the process of how and by whom audit and feedback processes are executed needs to be written down at a minimum. The transition to the Intermediate stage is that this is approved and made official by the nCSIRT management. The Advanced stage requires level 4, meaning that the audit process itself is subject to a regular assessment on the authority of higher levels of governance, and that there is active feedback following such assessments.

P-9 : EMERGENCY REACHABILITY PROCESS

Description: Describes how to reach the CSIRT in cases of emergency.
Clarification: Often only open to fellow teams.

GCMF Annotation:

P-9	Basic: 2	Intermediate: 3	Advanced: 3

The reachability of the nCSIRT is related to several organisational parameters like mandate (parameter O-1), constituency (parameter O-2), responsibility (parameter O-4), services (parameters O-5 and O-7), but also human parameters like having enough people at the job (parameters H-2) and tools parameters such as resilient phone, e-mail and internet access (parameters T-5 to T-7). National teams exchange information with their constituents and other stakeholders on a regular basis. But how can the nCSIRT be reached during times of crisis and emergency? For the senders of information, it is important to know through what modes of communication (e-mail, phone, website) they can contact the nCSIRT, and when: business hours, and how are those defined (including time zone information), or 24/7.

The Basic stage, requires at least level 2 because the nCSIRT's constituents and other actors have to be able to find the (emergency) contact details and information on the procedure to follow or expect. Level 2 means they can find this information in some service document or on a restricted-access webpage. If the information is publicly available online, or if the team is available 24/7 and publishes how they can be reached, then the level automatically goes to 3, as publication pre-supposes management approval.

For the Intermediate and Advanced stages, level 3 is required, as it is reasonable to assume that something as important as emergency reachability has been sanctioned by the nCSIRT's management.

P-10 : BEST PRACTICE E-MAIL AND WEB PRESENCE

Description: Describes (1) the way in which generic, security related mailbox aliases @org.tld are handled by the CSIRT or by parties who know when what to report to the CSIRT – and (2) the web presence.
Minimum Requirement:
(1) The handling of the following mailbox aliases (from RFC-2142 and best practice) is secured in such a way that the handlers either are part of the CSIRT or know the CSIRT, what it is for, and how to reach it when needed:
Security: security@ ; cert@ ; abuse@
E-mail: postmaster@
IP-numbers & domain names: hostmaster@
WWW: webmaster@ ; www@
(2) Some form of web presence for the CSIRT, at least internally. That presence must at least explain what the CSIRT is for, who it is for, and how it can be reached and when. Additional recommendations are (a) to link rfc-2350 from that presence, and (b) to enable a slash-security page, that is a page like www.org.tld/security, which can serve a wider security purpose than just the CSIRT.

GCMF Annotation:

P-10	Basic: 2	Intermediate: 2	Advanced: 2

An nCSIRT (or any other CSIRT) has to make sure that they can be found and contacted online (e-mail, web and social media presence). Communication is at the heart of any nCSIRT. National teams need to have a grip on how their online presence is organised, for example making sure they receive and process the information that is being sent to dedicated e-mail addresses and social media. This parameter is closely related to communication tools (especially parameters T-3, T-6 and T-7) and part of the content of P-10 will also found in a team's rfc-2350 (see parameter O-5).

The essential idea here is that for non-experts it is not at all easy "to find the right CSIRT" for a specific case (incident, threat, vulnerability). Usually, not even nCSIRTs are easy to find. Therefore, teams need to be very liberal at being reachable and open for incoming reports. Rfc-2142 (which is about 'common mailbox names') defines a series of e-mail addresses for

that purpose. Some of them the team may choose to publish (like security@ or cert@), but at least should the team be reachable via all those e-mail addresses, either directly or indirectly (through other colleagues in e.g. the host organisation who know how to find the team). This also expands for webpages and twitter and other social media channels that are used by the nCSIRT.

All 3 maturity stages require level 2 for this parameter, meaning that this has to be at least implemented and documented. To get formal management approval for this, which would make it level 3, is certainly feasible and logical, but not currently required for any of the maturity stages.

P-11 : SECURE INFORMATION HANDLING PROCESS

Description: Describes how the CSIRT handles confidential incident reports and/or information. Also has bearing on local legal requirements.
Clarification: it is advised that this process explicitly supports the use of TLP, the information sharing Traffic Light Protocol. (In the next version of SIM3 this advice will most likely become a requirement.)

GCMF Annotation:

P-11	Basic: 2	Intermediate: 3	Advanced: 3

The secure information handling process is important for nCSIRTs because they handle and store sensitive and confidential information. Sometimes they generate such information themselves because of monitoring activities, but nCSIRTs also receive such information from their constituency, other CSIRTs, or other (inter)national stakeholders. This process is about how the technical and organisational aspects of confidentiality are handled within the nCSIRT. Aside from the already mentioned handling and storage of information, this also extends to the security level of relevant applications, the screening of employees, the back-up system (including the security of off-site back-ups), and the support of the Traffic Light Protocol (TLP).

For the Basic stage it is still sufficient to be at level 2, meaning that the process has to be written down at least, and will typically be available on a team wiki or similar team information sharing facility. To deal with information (often with TLP designations) in a secure way and to assure the outside world that this is done responsibly, it is important to have explicit management approval for this. Therefore, the Intermediate and Advanced stages required to be at level 3. There is generally no urgent need for auditing this process from a

higher management level, as this is mostly an internal process. Therefore, level 4 is not required.

P-12 : INFORMATION SOURCES PROCESS

Description: Describes how the CSIRT handles the various information sources available to the CSIRT (as defined in the related tool, if available – see T-2).

GCMF Annotation:

P-12	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs often have various information sources at their disposal that they use to (better) provide services to their constituents. That list of information sources is the topic of parameter T-2. That list is already a valuable resource, but it also needs (a) a differentiation between the various sources in terms of trust and handling, and (b) maintenance of the list. Both of these should be part of the information sources process (that is thus connected with parameter T-2).

If there is no information sources process at hand, the CSIRT will not really know what kind of "trust" they invest in the various sources, and thus they will not know how to best handle each source. Nor will they have a system for maintenance of the list of sources, including a process that deals with the addition of new sources – and deletion of old ones. Without a proper P-12 process, especially newer members of the nCSIRT will be partially blind, may lend too much credibility to low quality sources, or too little urgency to highly trusted ones, and will therefore not be able to do their job well.

Therefore it is strongly recommended to have a well-considered information sources process, that includes a system of addition, maintenance and deletion of sources (going into the T-2 list). In addition it should include that for each of those sources there is some idea of how trustworthy the information is expected to be, how important it is to handle, and how it should be handled (as this will depend on the kind of source, and the type of information available there).

The requirements for the Basic to the Advanced stage increase from level 1, via 2, to 3. For the Basic stage it is important that team members know how to deal with sources and explain this to each other, as this knowledge usually derives from the more experienced team members. The Intermediate stage is entered when the process has been written down and made available on a team wiki or similar team information sharing facility. The Advanced stage

requires that the process has been formally approved by nCSIRT's management, and is being properly maintained.

P-13 : OUTREACH PROCESS

Description: Describes how the CSIRT reaches out to their constituency not in regard incidents but in regard PR and awareness raising.

GCMF Annotation:

P-13	Basic: 1	Intermediate: 2	Advanced: 3

The constituency of an nCSIRTs has to be made aware of the nCSIRT's existence and services offered. This needs to be done not just in the initial phase, but as an ongoing effort. Especially in times when not many incidents are visible it is easy for the public and even for relevant stakeholders to 'forget' about the topic of cybersecurity incident management, and those who are tasked to perform that. Be visible, stay visible. How to do just that is described in the outreach process: the ways and steps by which the nCSIRT advertises itself in order to raise its visibility and sustain and improve its reputation. Note that this process does not include the incident management related communications. Included in the outreach process can be awareness building activities such as conferences, trainings, workshops and webinars, blog posts, cybersecurity weeks, annual trend reports, press releases, and so on.

The requirements for the Basic to the Advanced stage increase from level 1, via 2, to 3. For the Basic stage it is important that team members simply perform outreach activities, agreeing inside the team on what needs to be done. The Intermediate stage is entered when the process has been written down and made available on a team wiki or similar team information sharing facility. The Advanced stage requires that the process has been formally approved by the nCSIRT's management, and is being properly maintained. This means that the outreach process has been institutionalised and is subject to quality control inside the team.

For this process in particular, it is well worth considering to aim for level 4, as outreach is so crucial that it would be very good to have it audited, and to discuss it with the higher governance levels. However, this is not currently required for any of the maturity stages.

P-14 : REPORTING PROCESS

Description: Describes how the CSIRT reports to the management and/or the CISO of their host organisation, i.e. internally.

GCMF Annotation:

P-14	Basic: 2	Intermediate: 3	Advanced: 4

nCSIRTs will always need to report facts and figures, and statistics about their performance to some higher level of governance, either inside their host organisation (ministry, agency, private entity, etc) or elsewhere. The reporting process will at least contain reporting on the numbers and types of incidents that were handled/coordinated (with extra attention for critical incidents), but the reporting process should also focus on other services performed by the nCSIRT, on issues of staff (hiring, training, etc), on resources (tools, means), and – if possible – also on situational awareness and threat levels. Lessons learnt should be an integral and explicit part of the reporting.

The requirements from the Basic to the Advanced stage increase from level 2, via 3, to 4. For the Basic stage it is sufficient to have a written process about how the reporting should work, made available on a team wiki or similar team information sharing facility: this way the team knows when to rapport what to who.

For nCSIRTs, reporting is especially important since it often includes reporting to parliament. In addition, Sunshine laws and other government processes that require transparency may come into play as well. As such, it is only logical that at the Advanced stage, level 4 is required for this parameter, making it subject to audits and feedback. The Intermediate stage then serves as step in-between, and needs to be at level 3: verified and approved by the nCSIRT's management.

P-15 : STATISTICS PROCESS

Description: Describes what incident statistics, based on their incident classification (see O-8), the CSIRT discloses to their constituency and/or beyond.
Clarification: If not applicable as in case of an explicit choice only to report internally, choose -1 as Level and will be omitted from "scoring".

GCMF Annotation:

P-15	Basic: 1	Intermediate: 2	Advanced: 3

nCSIRTs gather lots of data over time (on incidents as well as other data) and they report on this internally according to the reporting process (parameter P-14). This kind of reporting will naturally include statistics, graphs, pie-diagrams etcetera. A subset of those statistics may be suitable for publication to the team's constituency, to policy makers or politicians, or to the general public. P-15 is the process that describes what statistics the team gathers for

publication to their constituency and possibly to the world, and when and how they publish those statistics. With nCSIRTs, publication is often in the form of trend reports, usually on an annual basis. (P-15 is not about the statistics that are included in normal reporting: that is part of parameter P-14.)

nCSIRTs do not always publish statistics to their constituency or beyond. In those cases, it is possible to choose level 1 (meaning: not applicable), and P-15 will then then be omitted in the assessment of the overall maturity level (Basic, Intermediate and Advanced stages).

The requirements for the Basic to the Advanced stage increase from level 1, via 2, to 3. For the Basic stage it is important that team members know what statistics to publish, to who and when, agreeing inside the team on what needs to be done. The Intermediate stage is entered when the process has been written down and made available on a team wiki or similar team information sharing facility. The Advanced stage finally requires that the process has been formally approved by team management, and is being properly maintained, meaning that the statistics process has institutionalised and is subject to quality control inside the team – which is where you want to go for an important process like this one, that could cause reputational damage when badly performed.

Sometimes, the publication of statistics is mandated in national law. Where that is the case, level 4 applies for this parameter.

P-16 : MEETING PROCESS

Description: Defines the internal meeting process of the CSIRT.

GCMF Annotation:

P-16	Basic: 1	Intermediate: 1	Advanced: 2

For all CSIRTs including national ones it is essential to have regular internal team meetings. Team meetings are often weekly, and are often short and focused. The aim is to review important incidents and threats, to see what went well, but especially what went less well, and to learn from that together. Lessons learnt are great opportunities for improvement and may lead to adaptation of processes, proposals to follow specific trainings, research into new/better tools, and so on. Team meetings are an integral and essential part of the work hygiene and quality control process of the nCSIRT.

Of course, the size of the team will influence the shape and organisation of the team meetings. Smaller teams can more easily meet with open agendas, bigger teams will need more

structure. In all cases, it is important that all participants of the meeting feel free and encouraged to contribute, and to also share bad news and critique. An encouraging attitude of the team leaders and management is essential to make this succeed, and a critical, constructive attitude should be rewarded rather than grudgingly accepted. This meeting aspect is crucial as the CSIRT work is never the same – there are continuous changes in the threat landscape, continuously new, or adapted attacks, unexpected incidents, and so on. A CSIRT can never rest on its laurels, they need to be vigilant and open to learning all the time.

Some teams also use the team meetings for short presentations by team members on a specific topic that they have been devoting their attention to, or about a training they just received, etcetera. Of course, the aim then is to be flexible, but to encourage all team members to share like this during the year. This can also contribute to team building.

For the Basic and Intermediate stage, it is enough to be at level 1. Having these meetings and learning from them is what really counts, and what is more important than writing down the process (although that is also quite simple). For the Advanced stage it is enough if there is an informal write-up of the process, being level 2, which can be as simple as: "the incident response team meets every week on Monday morning from 10 to 11, to discuss the preceding week, and formulate action points and lessons learnt to take into account on short term and longer term, with the support of the management".

The nCSIRT management needs to support the meeting process, and especially with smaller teams, engage in them from the start. This could lead to a level 3 process, although this is not seen as a requirement in terms of the maturity stages: what is essential is to have those meetings, take the learnings, and act on them.

P-17 : PEER-TO-PEER PROCESS
Description: Describes how the CSIRT works together with peer CSIRTs and/or with their "upstream" CSIRT.

GCMF Annotation:

P-17	Basic: 1	Intermediate: 2	Advanced: 2

It is useful to first note that an nCSIRT will rarely, if ever, have an "upstream" CSIRT: it is of paramount importance that nCSIRTs can freely roam and communicate inside the national, regional and global CSIRT community.

It is important for all CSIRTS to be a member of relevant CSIRT communities in order to foster trust relationships with other teams. For nCSIRTs this is arguably even more essential. They have a national responsibility and do not really have the option nor authority to just "isolate" the country or take other draconic measures. In order to perform their duties, nCSIRTs must work together with other national teams, but also with other CSIRTs, critical vendors (and their PSIRTs), and suppliers of threat intelligence. This has been explained more under parameter O-9, and the human aspect under parameter H-7.

As a result, the nCSIRT will participate in at least one, but usually more "cooperations" of CSIRTs/PSIRTs, by memberships or associations. Sometimes, teams also sign Memoranda of Understanding (MoUs) with other teams that are relevant for them to collaborate with. The other teams in such cooperations, or the other party/parties in the MoU are labelled as "peer teams" or simply "peers". Thus, all FIRST members together form a group of peers. All TF-CSIRT accredited/certified teams are a group of peers. Same for APCERT members, and so on, all CSIRT cooperations have their own group of members. The group of teams that signed an MoU together are peers. Inside a country, the nCSIRT will likely have peer relationships with sectorial CSIRTs and critical infrastructure teams.

In all cases, a group of peers will have special ways of working together, and they may be able to use restricted websites together, or even shared tools. The levels of trust will differ between the different peer groups. CSIRTs who are not a peer in any of those groups, may be "less trusted" by default. For nCSIRTs, politics will also enter the scene: an nCSIRT is more likely to closely work together with nCSIRTs of countries they have close relationships with, or countries who are members of the same economic cooperation, than with countries who have very different characteristics. As this landscape can become quite confusing, especially for members of the nCSIRT in their daily work, it is important that the team is aware of the various kinds of peers, and what level of trust and special procedures apply to which group of peers. This is the peer-to-peer process.

At the Basic stage, level 1 is required, which shows that there is no need to immediately formalise or write down the peer-to-peer process at the start. The process should be known by the people who are tasked to perform it. However, it is problematic to discuss and train team members on a process that has not been written down. Therefore, level 2 is required for the Intermediate and Advanced stages. This is typically a process that is detailed, listing the different peer groups and the trust levels, procedures, websites and possibly tools associated with those peer groups. The process will be placed on a team wiki or similar team information sharing facility. It is certainly worthwhile to go beyond level 2, but not currently required for the Advanced stage.

Working Group B | Taskforce Cyber Incident Management