Global CSIRT Maturity Framework

Stimulating the development and maturity enhancement of national CSIRTs

Version 1.0 | June 2019

Global CSIRT Maturity Framework

Stimulating the development and maturity enhancement of national CSIRTs

Authors: Hanneke Duijnhoven (TNO), Tom van Schie (TNO) and Don Stikvoort (S-CURE)

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 CSIRT Maturity Framework is aimed at parties involved in planning, building and leading such capacities.

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

[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.

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	**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 (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 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.

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, divided over 4 categories:

O: Organisational
H: Human
T: Tools
P: Processes

A parameter is an attribute relevant for the operationalisation and functioning of a CSIRT. Each parameter can be measured on a scale of 0 to 4 (see Table 2).

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 the national CSIRTs in the European Union. [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 [11]. ENISA's tool aims at national CSIRTs [12].

Table 2 – 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

The 44 parameters are listed in Table 3. The full details for all parameters are given in Appendix A.

Table 3- 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

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.

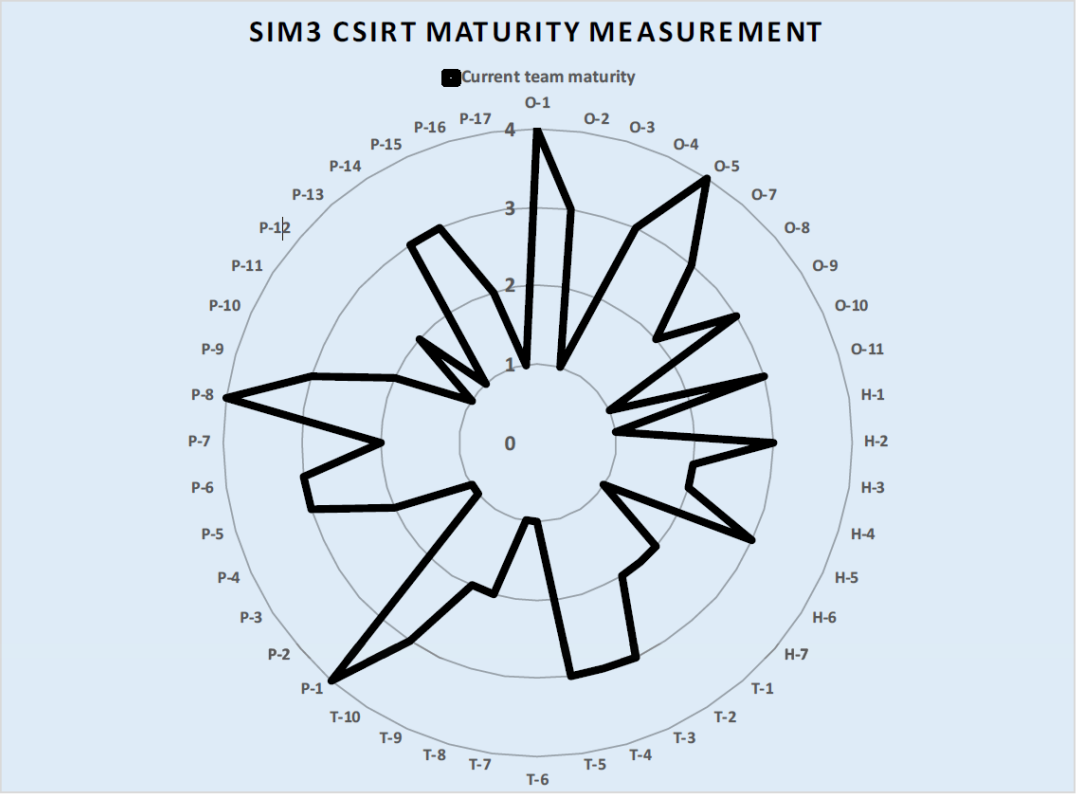


Figure 1: CSIRT maturity assessment example outcome

CSIRT Maturity stages

This chapter 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. For instance, one of the essential qualities of national CSIRTs is to set-up meaningful collaborations in their complex national constituencies, and to be *organised* in such a way as to enable this. Consequently, for all maturity stages, the organisational parameters need to score relatively high. As another 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.

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 regards 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.

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.

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 European "CSIRTs Network" members use a combination of self-assessment and peer reviews to improve their maturity. [6]

Assessments can also be 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].

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://www.thegfce.com/initiatives/c/csirt-maturity-initiative/documents/publications/2017/11/21/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 (http://www.csirtnetwork.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 “Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity” (https://www.enisa.europa.eu/publications/study-on-csirt-maturity)
   For the ENISA CSIRT maturity assessment methodology, see the “Study on CSIRT Maturity – Evaluation Process” (https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process)

7. FIRST CSIRT Services Framework: https://www.first.org/education/csirt_services_framework
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://check.ncsc.nl/static/CSIRT_MK_guide.pdf
    Note: this reference will be updated in June 2019
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 – SIM3 description

Reprint[6] of the most relevant parts of the current version of SIM3, version mkXVIIIc (30 March 2015, updated 1 Sep 2018 & 1 May 2019) – see https://opencsirt.org/maturity/sim3/ for the latest version.

SIM3 : Security Incident Management Maturity Model

Basic SIM3

The maturity model is built on three basic elements:

1) Maturity parameters
2) Maturity clusters
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.

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)

[6] This reprint was authorised by the Open CSIRT Foundation, as were the “cuts” from the original.

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:

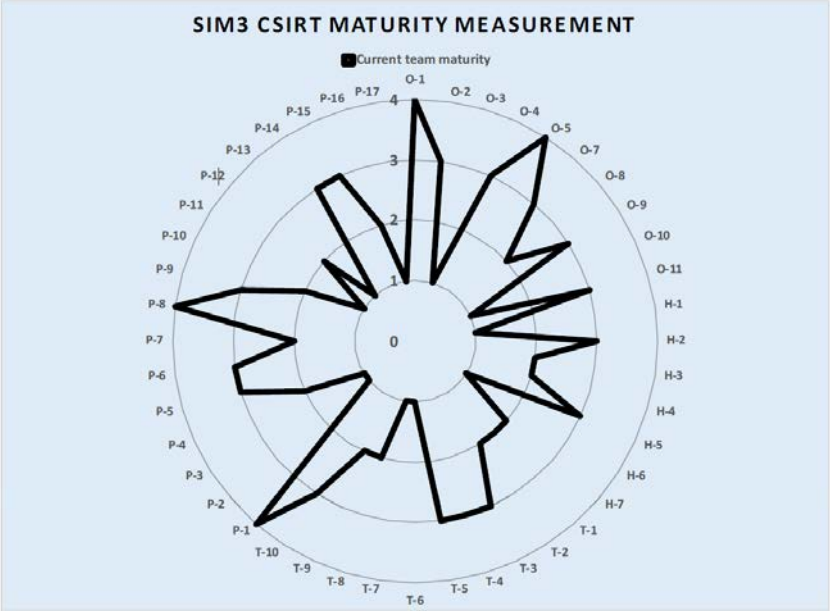
0 ➔ 1 : addition of *consideration* - "listen, we are aware of this"
1 ➔ 2 : addition of *written description* - "read, this is the way we do it"
2 ➔ 3 : addition of *accountability* - "look, this is what we are bound to do"
3 ➔ 4 : addition of *control mechanism* – "and this is how we make sure that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

O-1 : MANDATE
Description: The CSIRT’s assignment as derived from upper management.

O-2 : CONSTITUENCY
Description: Who the CSIRT functions are aimed at – the “clients” of the CSIRT.

O-3 : AUTHORITY
Description: What the CSIRT is allowed to do towards their constituency in order to accomplish their role.

O-4 : RESPONSIBILITY
Description: What the CSIRT is expected to do towards their constituency in order to accomplish their role.

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.

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.

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.

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).

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.

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.

H – “Human” Parameters

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[7]. 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.

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.

H-3 : SKILLSET DESCRIPTION
Description: Describes the skills needed on the CSIRT job(s).

H-4 : INTERNAL TRAINING
Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones.

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.)

H-6 : (EXTERNAL) COMMUNICATION TRAINING
Description: Program to allow staff to get (human) communication/presentation training externally.

H-7 : EXTERNAL NETWORKING
Description: Going out and meeting other CSIRTs. Contributing to the CSIRT system when feasible.

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.

T-2 : INFORMATION SOURCES LIST
Description: Where does the CSIRT get their vulnerability/threat/scanning information from.

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.

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.

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

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 fallback mechanism for when a team's landlines are out of order.
Minimum requirement: Fallback mechanism for the case of phone system outages

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.

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.

T-8 : INCIDENT PREVENTION TOOLSET
Description: A collection of tools aimed at preventing incidents from happening in the constituency. The ' 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".

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.

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.

P – "Processes" Parameters

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.

P-2 : ESCALATION TO PRESS FUNCTION
Description: Process of escalation to the CSIRT's host organisation's press office.

P-3 : ESCALATION TO LEGAL FUNCTION
Description: Process of escalation to the CSIRT's host organisation's legal office.

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.

P-5 : INCIDENT DETECTION PROCESS
Description: Describes how the CSIRT detects incidents, including the use of the related toolset.

P-6 : INCIDENT RESOLUTION PROCESS
Description: Describes how the CSIRT resolves incidents, including the use of the related toolset.

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.

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.

P-9 : EMERGENCY REACHABILITY PROCESS
Description: Describes how to reach the CSIRT in cases of emergency.
Clarification: Often only open to fellow teams.

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.

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 this document this advice will most likely become a requirement.)

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).

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.

P-14 : REPORTING PROCESS
Description: Describes how the CSIRT reports to the management and/or the CISO of their host organisation, i.e. internally.

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”.

P-16 : MEETING PROCESS
Description: Defines the internal meeting process of the CSIRT.

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

Working Group B | Taskforce Cyber Incident Management