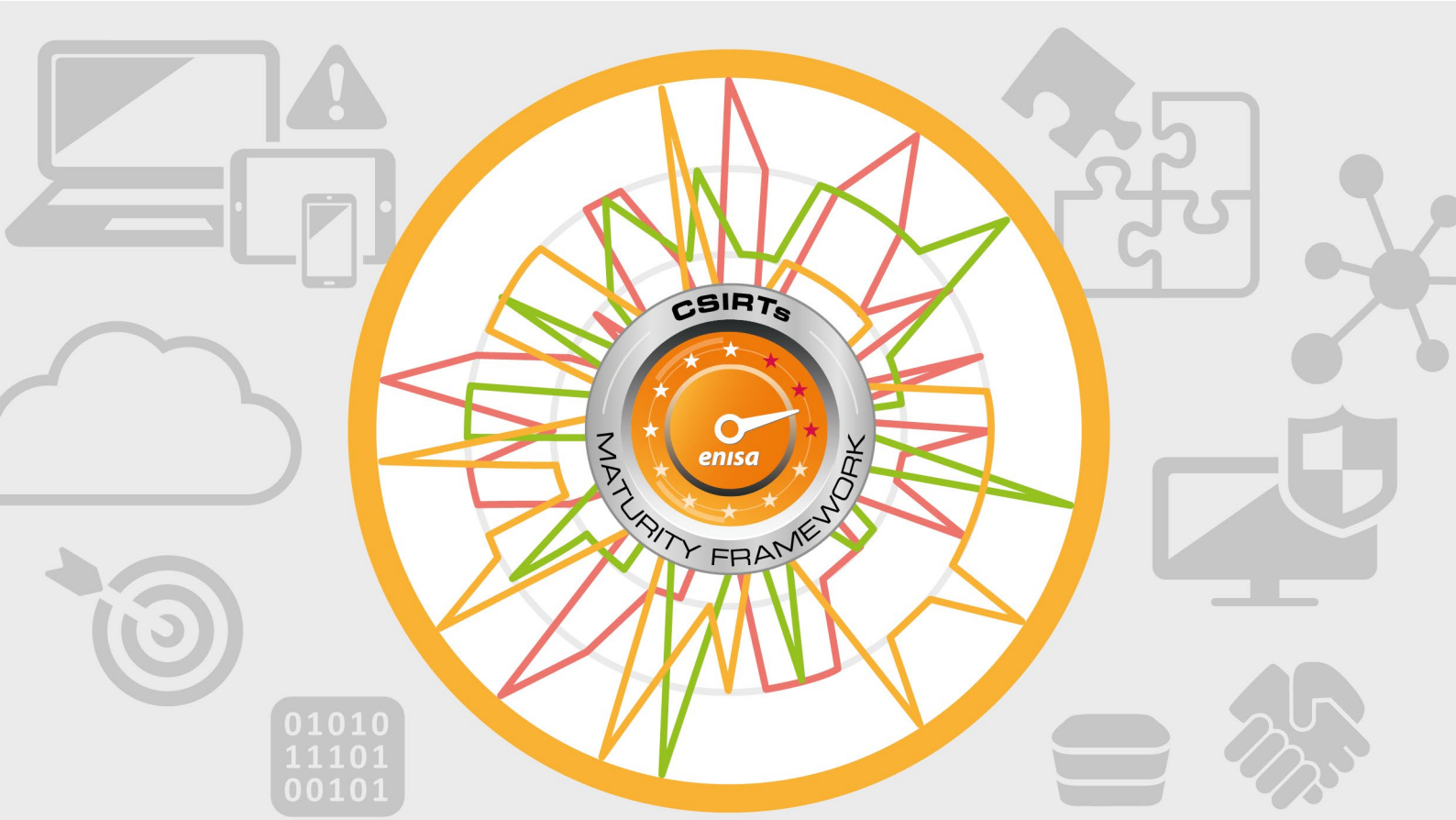
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENISA CSIRT MATURITY FRAMEWORK

Updated & Improved

FEBRUARY 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, co-operates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors please use ocu@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Andrea Dufkova (ENISA), Don Stikvoort (Open CSIRT Foundation), Klaus Peter Kossakowski (University of Hamburg), Miroslaw Maj (ComCERT), Vilius Benetis (NRD Cyber Security) and Kamil Gapinski (ComCERT)

ACKNOWLEDGEMENTS

Stichting Open CSIRT Foundation, CSIRTs Network Maturity Working Group members, Olivier Caleff (SIM3 auditor), Edgars Taurins (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-563-0, DOI 10.2824/35453 Catalogue Number TP-07-22-077-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The ENISA CSIRT Maturity Framework is intended to contribute to the enhancement of the global capacity to manage cyber incidents, with a focus on CSIRTs. Cyber incidents and developments are inherently transnational and effective responses depend on transnational collaboration. The establishment of national CSIRTs[1] is an essential step to facilitate the building of cyber capacity both within and across nations and make it more effective. The ENISA CSIRT Maturity Framework is aimed at parties involved in planning, building and leading such capacities with a concrete focus to increase maturity of all CSIRTs in the CSIRTs Network[2].

The ENISA CSIRT Maturity Framework is built on three pillars:

1. the well-established OCF SIM3[3] standard;
2. the ENISA three-tier maturity approach: a series of three pre-defined steps that can be used as a guideline for the steps to be taken to increase maturity, complete with practical guidance on how to work with the Maturity Framework at different phases – from pre-establishment to advanced levels of maturity;
3. the ENISA assessment methodology: self-assessment and peer-reviews applied in the CSIRTs Network.

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 the capacity to respond to cyber incidents. However, the steps to maturity that have been defined are based on extensive experience and expertise in the CSIRT community and offer valuable guidance for national CSIRTs with regards to the level of quality to which they aspire. The CSIRT Maturity Framework combines previous models that have been widely recognised and adopted.

In this document the updated and improved version of the Framework is presented. This includes changes to all three pillars mentioned above.

1. Some aspects of SIM3 have been improved upon, and brought up to date – leading to a strong recommendation to OCF[4] to include these in any new drafts of the SIM3 standard.
2. The three-tier maturity approach has remained the same as regards terminology, including the terms Basic, Intermediate and Advanced. However the demands on those three steps have been upgraded, in line with the development of the maturity of the CSIRTs Network in the past four years while also reflecting the changing landscape of the NIS Directive5.
3. The self-assessment and peer-review system received a complete overhaul, with in-depth guidance, which is expected to not only make this process easier to work with, but also lead to higher quality and more consistent results.

[1] The term 'National CSIRT' is more closely defined later in the report.
[2] https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network
[3] http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf
[4] https://opencsirt.org/
[5] https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

1. INTRODUCTION

This document presents ENISA's Computer Security Incident Response Teams (CSIRT) Maturity Framework that is intended to contribute to the enhancement of the capacity to manage cyber incidents, with a focus on national CSIRTs[6]. It is aimed at parties involved in planning, building and leading such capacities. This document has been developed as part of ENISA's continuous commitment to enhancing CSIRTs and related methodologies.

National CSIRTs play a crucial role in the collaboration and co-ordination between national and international communities and organisations. Cyber incidents and developments are inherently transnational and effective responses depend on transnational collaboration. The establishment of national CSIRTs is an essential step to facilitate and co-ordinate the building of cyber capacity 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. As such, CSIRTs form an essential element of cyber incident management and cyber capacity in general.

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 or 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 CSIRT has an external focus and provides services to a sector or nation, and usually has a limited mandate to access or implement security measures within the actual IT systems of their constituency. Therefore, these focus more on the co-ordination of responses, 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 co-ordinated responses to cyber incidents 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 links 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 CSIRTs 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 co-ordination 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 more teams. In cases of multiple national teams, it is important that the mandate and constituencies for each team are clearly defined and that they can co-operate closely.

Encouraging the establishment, expansion and maturity of national CSIRTs contributes to the ambition of building European and global cyber capacity, supplementing the existing network of

CSIRT MATURITY

Encouraging the establishment, expansion and maturity of national CSIRTs contributes to the ambition of building European and global cyber capacity, supplementing the existing network of private industry and academic and research CSIRTs.

[6] This document uses the term 'national CSIRT' to refer to a range of national cyber (co-ordination and response) activities, including CIIP, sectorial and governmental teams. Depending on the context, a national CSIRT can have a different focus or name. Currently the scope relates to CSIRTs Network (https://csirtsnetwork.eu/) as governed by the NIS Directive.

private industry and academic and research CSIRTs. To do so, it is important to approach the development of this network from both a technical as well as a policy perspective. Existing models and good practices for CSIRTs and CSIRT maturity can not only support nations that are ready to establish a national CSIRT but also nations that want to enhance the maturity of their national team.

The new version of the ENISA CSIRT Maturity Framework presented here includes the OCF SIM3 standard, with its more-than-forty parameters; the ENISA three-tier approach, which consists of three pre-defined maturity steps (Basic, Intermediate and Advanced) that can be used as stepping stones towards increased maturity; and an enhanced ENISA assessment methodology, based on a system of self-assessments and peer-reviews with elaborate guidance on best practice. A main thread in all this is to give guidance on how to work with the Maturity Framework with teams at different phases, from pre-establishment through the whole maturity cycle to the advanced stage.

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 capacity for responding to cyber incidents. However, the maturity steps that have been defined are based on extensive experience and expertise in the CSIRT community and offer valuable guidance for national CSIRTs regarding the quality level to which they aspire. It needs to be stressed here that the NIS Directive has been taken right from the start as the inspiration and guide for the steps towards maturity, and this is reflected in the ENISA three-tier approach – and with the changes in the NIS Directive, it became necessary to further upgrade the Basic, Intermediate and Advanced steps.

The ENISA CSIRT Maturity Framework builds on its previous incarnation and continues to adopt the Open CSIRT Foundation's SIM3 standard, whilst applying improvements and updates across the board.

Open CSIRT Foundation (OCF) – SIM3 [7]

SIM3 is designed as a generic maturity standard that applies to all types of CSIRTs, including national CSIRTs. The Open CSIRT Foundation (OCF) shepherds the development of SIM3.[8] The current version of SIM3 (latest update: May 2019) is popularly referred to as 'v1'. In the work that led to this new framework, done in co-operation with OCF, it was recognised that some changes and updates were needed; these will be reflected in an interim version of 'SIM3 v2' to be made available by the OCF. More information regarding this is found in Appendix E.

ENISA previous maturity framework: 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.

This tiered maturity approach is globally applicable, as was proven by the publication of the GFCE's GCMF or Global CSIRT Maturity Framework (April 2021) which, content-wise, is identical to the ENISA approach.

In Section 3 the maturity standard and maturity steps are presented. In Section 4, there is extensive guidance on the assessment methodology for the CSIRTs Network (self-assessments and peer-reviews).

[7] See http://opencsirt.org/csirt-maturity/sim3-and-references/
[8] The OCF encourages ENISA 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 and update SIM3.

1.1 DEPRECATION STATEMENT

The following documents are deprecated following the publication of this Framework:

1. ENISA Maturity Evaluation Methodology for CSIRTs, April 09, 2019, https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
2. ENISA CSIRT maturity assessment model, April 30, 2019, https://www.enisa.europa.eu/publications/study-on-csirt-maturity
3. Maturity Reference for CSIRTs – Executive Summary, January 15, 2018, https://www.enisa.europa.eu/publications/maturity-reference-for-csirts-2013-executive-summary
4. CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs, January 11, 2016, https://www.enisa.europa.eu/publications/csirt-capabilities
5. CSIRT Maturity - Self-assessment Tool, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-survey
6. CSIRTs Network internal documents (not publicly available)

2. ENISA CSIRT MATURITY FRAMEWORK

At the core of the ENISA CSIRT Maturity Framework lies the SIM3 standard, ENISA's three-tier maturity approach and its application in the form of self-assessments and peer-reviews. In this chapter both SIM3 and ENISA's three maturity steps are presented, in such a way that they can be applied globally.

2.1 3.1 SECURITY INCIDENT MANAGEMENT MATURITY MODEL (SIM3)

SIM3 stands for Security Incident Management Maturity Model and has been in use since 2008[9]. The maturity standard has been applied by teams all over the world, including various national CSIRTs[10]. 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. The current version of SIM3 is mkXVIIIc[11]. I was most recently updated in May 2019. It is in essence still the original SIM3, also known as 'v1'. Work on a new version, SIM3v2 is in process.

For the development of the new ENISA Framework, ENISA and OCF have co-operated to ensure that there will be no loss of synchronicity between the ENISA Framework and OCF's SIM3. In fact under the current ENISA project for updating the ENISA Framework, the updated SIM3 parameters will continue to align with SIM3v2.

Reference will be made to an interim draft version of SIM3v2 which is *as much as possible,* and indeed to a great extent, identical to SIM3v1 yet includes various updates, improvements and a few extensions that are necessary for both ENISA and OCF. The final version of SIM3v2, expected to be published by OCF late in 2022, will be more elaborate yet will not in any way invalidate the new ENISA Framework; both will remain fully compatible.

Below we refer to SIM3v2i – with 'i' referring to 'interim'. This can be replaced by just SIM3v2 once that has been finalised by OCF.

SIM3v2i features forty-five parameters, one more than SIM3v1. Parameters are attributes relevant for either the organisation, operation or functioning of a CSIRT.

The SIM3v2i parameters are divided into four 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's staff (this refers not only to technical staff but to all 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.

[9] The Open CSIRT Foundation (OCF) governs and maintains SIM3, and trains and certifies SIM3 auditors.
[10] Two online measurement tools exist. The OCF tool aims at all sorts of CSIRTs worldwide, including national ones. ENISA's tool aims at national CSIRTs.
[11] See http://opencsirt.org/csirt-maturity/sim3-and-references/

T: Tools
The tools ('T') parameters refer to the tools and technologies that are used by the CSIRT to reach its objectives and offer its services to its 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 or 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 categories (Organisation, Human and Tools), where the description or list is found more in those other categories, and the P-parameters focus on the steps that need to be taken.

The forty-five parameters are listed below in Table 1.

Table 1- Overview of SIM3v2i parameters [12]

Parameter number	Parameter description	Parameter number	Parameter Description
O-1	Mandate	T-6	Resilient Messaging
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-6	Public Media Policy	P-1	Escalation to Governance Level
O-7	Service Level Description	P-2	Escalation to Press Function
O-8	Incident Classification	P-3	Escalation to Legal Function
O-9	Participation in CSIRT Systems	P-4	Incident Prevention Process
O-10	Organisational Framework	P-5	Incident Detection Process
O-11	Security Policy	P-6	Incident Resolution Process
H-1	Code of Conduct/Practice/Ethics	P-7	Specific Incident Processes
H-2	Staff Resilience	P-8	Audit & Feedback Process
H-3	Skillset Description	P-9	Emergency Reachability Process
H-4	Staff Development	P-10	Best Practice Internet Presence
H-5	Technical Training	P-11	Secure Information Handling Process
H-6	Soft Skills Training	P-12	Information Sources Process
H-7	External Networking	P-13	Outreach Process
T-1	IT Assets & Configuration	P-14	Governance Reporting Process
T-2	Information Sources List	P-15	Constituency Reporting Process
T-3	Consolidated Messaging System(s)	P-16	Meeting Process
T-4	Incident Tracking System	P-17	Peer Collaboration Process
T-5	Resilient Voice Calls		

When working with the SIM3v2i framework, each parameter can be measured on a scale of 0 to 4 (see Table 2 below).

[12] O-6 is a new parameter introduced in SIM3v2. In SIM3v1 O-6 was intentionally left blank. All 44 other parameters have only had relatively minor name changes when changing from v1 to v2, in order to bring them up-to-date.

Table 2 – SIM3v2i parameter measurement scale

Level	Status	Indicators
0	Not available / undefined / unaware	-
1	Implicit	Known or 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 procedure for evidence could be) may be helpful:

Level 0 (Not available / undefined / unaware)

This score is mostly only met with teams made up of novices, as it means that the team members *have not yet thought* 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 teams of novices 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 conducting 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 down the content for this parameter, so as to increase consistency within the team – and also to make 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 that all CSIRTs have facilities like this as they provide an easy way to bring the most important processes, tools (and manuals) and policies under the direct attention of those doing the work of incident management. A wiki-style approach has the added advantage of allowing hyperlinks, thus enabling the internal information to be easily structured and interconnected; e.g. 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 other cases that can lead to a level 2 score such as, 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. For 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 characteristic 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, but for most information it is advisable that, at some stage, what has come to be the consensus is 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 to any parameter where the subject matter of that parameter has been formally and explicitly (in 'writing') approved by the team management. Here we mention a few of the most common situations for level 3.

1. 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, 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 into team operations and information systems to ensure that team members actually know of 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 a team's internal documents.
2. 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 team operations and information systems to ensure that the team members actually know of and use them.
3. Wiki-style level 2 information or pages or documents that are 'upgraded' to level 3: this of course requires explicit (visible) authorisation by team management for such 'pages'. It is currently not demanded by SIM3 but it is highly recommended to go one step beyond this and not just grant authorisation, but also include some system of expiry and maintenance for such pages. Some wiki-types have facilities or plug-ins to make this 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 for the team but has the active attention of some higher governance level above the team's management. There needs to be evidence of this, and this evidence must include the following.

1. There must be a process of checking, assessing or auditing 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 two years and usually once a year.
3. The process must be 'active,' which means in that there is a feedback mechanism towards the team management (and the team) in addition to the process of checking and reporting on it. This feedback mechanism is intended to ensure that there is communication about the parameter between the 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 levels and the team in order to enable improvements: clearer policies, better tools and processes, more people, better training sessions and education, etc.

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

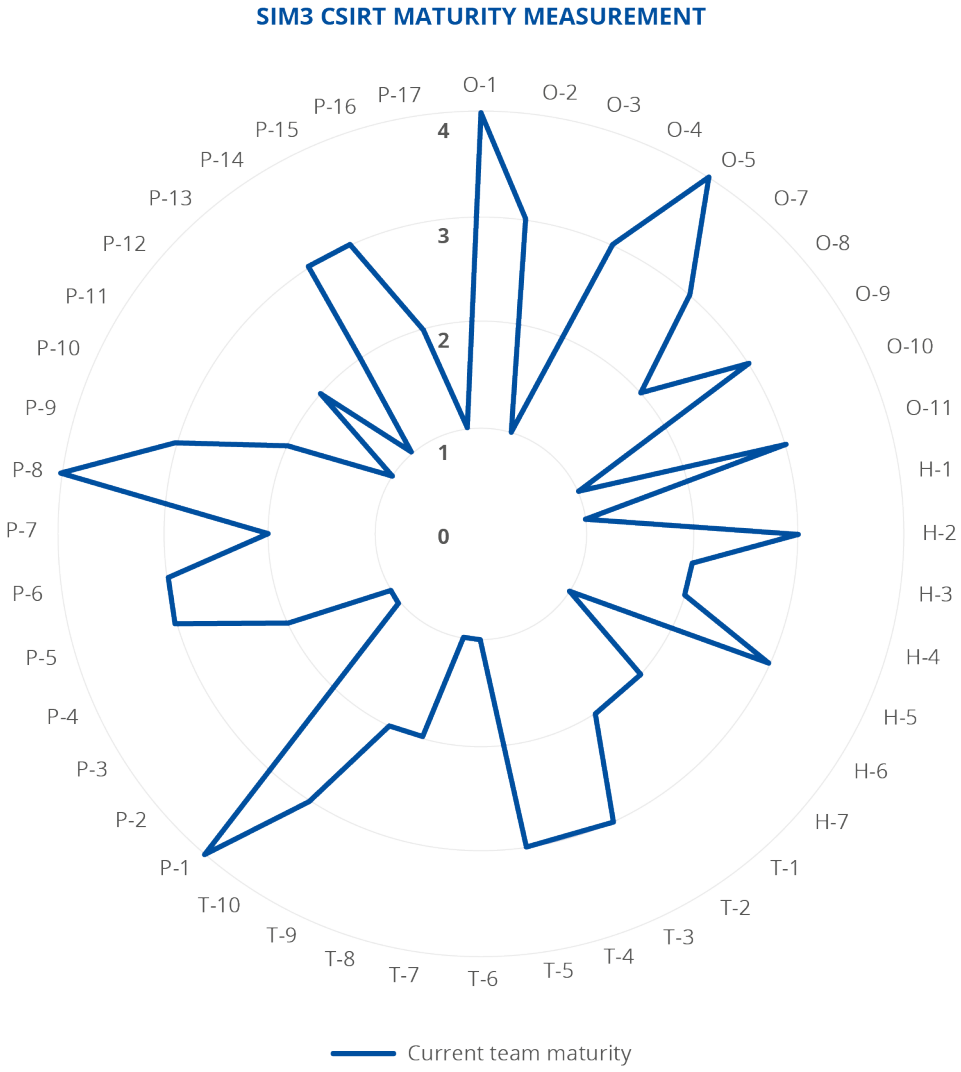
1. When the topic of a parameter is formally and unambiguously part of the national cyber (security) legislation, that parameter automatically scores level 4, because it is assumed that the system of legislation and the checks and balances associated with that are more than sufficient to warrant level 4. It is, however, important to note here that the mere mentioning of something in the law – even if it is clear and unambiguous – still requires the team to implement this internally so as to be able to effectively 'make the law work'. So such aspects still require documentation inside the team, by being embedded in a team information system (e.g. team wiki), integrated into internal training, etc.
2. When there is a team organisational framework, charter or a 'team handbook' (O-10), it is strongly advised to have a paragraph there for the team about the assessments or audits, which is essentially the P-8 parameter process. This should include internal team assessments (which alone 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, acknowledging their independent position is recommended while requesting 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, such as H-2, P-1 and P-2.

In other cases, it is often harder to find clear *evidence* for level 4 characteristics when, for instance, an auditing department does an extensive audit of the nCSIRT every year and they use SIM3 as one of the controlling documents but no-one has written down some minimal requirements for that audit. In such a case, alternative evidence can be a posteriori rather than a priori; meaning, a few of those audit reports may be reviewed to see what they contain in order to gauge whether it is reasonable to assume that a certain SIM3 parameter was indeed audited in a 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 forty-five parameters[13] are given a score and the figure provides visual insight of the maturity of a team.

[13] The new parameter O-6 is still missing in this example figure.

Figure 1: CSIRT maturity assessment example outcome



2.2 CSIRT MATURITY STEPS – THREE-TIER APPROACH

This paragraph provides information on the maturity steps that can be used to assess the maturity of a national CSIRT and support decision-making on where to focus efforts to increase maturity. The maturity steps previously developed by ENISA are the three-tier maturity approach. Three steps have been defined: *Basic*, *Intermediate* and *Advanced*. An *Under-basic* step is designated to those who do not yet reach the requirements of the *Basic* step.

For each step, a minimum value is assigned for each of the forty-five parameters. The values for each parameter at each of the three steps are based specifically on the profile requirements for most national CSIRTs. This means that, in practice, some parameters will be more relevant for some national teams than for others – the weighting of that is the responsibility of the teams in question.

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* step national CSIRTs 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 steps, none of these parameters requires a level higher than level 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 these parameters achieving level 4 – but in general such a level is not required for the three maturity steps for national CSIRTs. As a final example, most national CSIRTs will play less of a role in the prevention of an actual incident and therefore the value for T-8 (Incident Prevention Toolset) and P-4 (Incident Prevention Process) are low across all three maturity steps.

The *Basic* and *Advanced* steps allow national CSIRTs to define a growth path. New teams can first aim to achieve the *Basic* step in the 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 – note here that the peer-review cycle in the ENISA Framework uses change-cycles of up to 3 years.

The *Intermediate* step offers some guidance for setting a path for growing from *Basic* towards *Advanced*, although – depending on specific needs – some teams may opt to develop right from Basic to Advanced. The higher steps are in place to show that a national team has reached a higher level of maturity and that the conditions that enable interaction with CSIRTs worldwide reactively as well as pro-actively have been met. It will also facilitate the building of trust between teams. Below, a short explanation of the three steps is provided.

2.2.1 Under-basic step

The Under-basic step applies to CSIRTs who have not yet reached the *Basic* step for one or more parameters. This step is especially relevant for teams who want to secure resources to improve their maturity and move to higher steps.

2.2.2 Basic step

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 must already have a good foundation with 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* step; 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.

2.2.3 Intermediate step

This step builds on the Basic step 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* step, without such controls. In the other categories (human, tools and processes) there is also gradual progress on most parameters.

2.2.4 Advanced step

For national CSIRTs to progress from merely ‘working together’ on handling incidents to establishing a comprehensive co-ordinated capacity to manage incidents, including effectively

and reliably sharing threats, vulnerabilities and early-warning data with 'peer' national CSIRTs[14], it is essential that these teams reach a high level of maturity. The parameter values for the *Advanced* step 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 minimum scores required for the three maturity steps are specified in Table 3 below. Appendix E presents a version of the table below that highlights the changes between the current ENISA Framework and the new one (and thus also the changes between SIM3v1 and SIM3v2i), and also indicates what the increase has been in the overall maturity demands for the three steps.

Table 3 - Overview of ENISA maturity steps with minimal SIM3v2i score for each parameter

Parameter number	Parameter description	Minimum values for the tiers:		
		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-6	Public Media Policy	2	3	4
O-7	Service Level Description	3	4	4
O-8	Incident Classification	2	3	3
O-9	Integration in CSIRT Systems	3	4	4
O-10	Organisational Framework	3	3	3
O-11	Security Policy	2	3	4
H-1	Code of Conduct/Practice/Ethics	2	3	3
H-2	Staff Resilience	2	3	4
H-3	Skillset Description	2	2	3
H-4	Staff Development	2	3	4
H-5	Technical Training	1	2	3
H-6	Soft Skills Training	1	2	3
H-7	External Networking	2	3	3
T-1	IT Assets & Configurations	1	2	3
T-2	Information Sources List	2	3	4
T-3	Consolidated Messaging System	2	3	3
T-4	Incident Tracking System	2	3	3
T-5	Resilient Voice Calls	2	3	3

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

T-6	Resilient Messaging	2	3	3
T-7	Resilient Internet Access	2	3	3
T-8	Incident Prevention Toolset	2	2	3
T-9	Incident Detection Toolset	2	3	3
T-10	Incident Resolution Toolset	2	3	3
P-1	Escalation to Governance Level	3	4	4
P-2	Escalation to Press Function	2	3	3
P-3	Escalation to Legal Function	2	3	3
P-4	Incident Prevention Process	2	3	4
P-5	Incident Detection Process	2	3	4
P-6	Incident Resolution Process	2	3	4
P-7	Specific Incident Processes	2	3	4
P-8	Audit & Feedback Process	3	4	4
P-9	Emergency Reachability Process	2	3	3
P-10	Best Practice Internet Presence	2	3	3
P-11	Secure Information Handling Process	2	3	3
P-12	Information Sources Process	2	3	4
P-13	Outreach Process	2	3	4
P-14	Governance Reporting Process	3	4	4
P-15	Constituency Reporting Process	2	3	3
P-16	Meeting Process	2	2	3
P-17	Peers Collaboration Process	2	3	4

2.3 3.3 ASSESSMENT METHODOLOGY

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 these 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 each 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 and 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 resources if the constituency of the national team is limited to the critical infrastructure sectors compared to when it also includes, for example, all companies and citizens.

2.3.1 Self-Assessment

The CSIRT Maturity Framework makes it possible to assess the maturity of a CSIRT through a self-assessment as the first step. Self-assessment can be useful for setting a baseline (more subjective) score for internal review purposes. It can also be used as the starting point to enhance maturity. Based on the self-assessment score, an action plan (including timeline) may be defined to improve to a higher level of maturity. Assessments can also be used to compare with peer CSIRTs using the Maturity Framework as guideline. The maturity steps defined in the CSIRT Maturity Framework are set as good practice to provide guidance for national CSIRTs. Some parameters may be less relevant to a specific team whilst others are at the core of their strategy.

2.3.2 Peer-Review

The second step in the assessment described in the CSIRT maturity framework is peer-review. 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 the assessment of CSIRT maturity.

After the team has done their self-assessment, the peer-reviewer can meet them – experience teaches that such a meeting is most effective when done on site – and discuss their results. This is a win-win situation where both sides can learn from each other. It will help the team to make their self-assessment more accurate (with an element of objectivity) and show how to effectively increase maturity. It also contributes to a level of trust between the teams for future collaboration.

Peer-reviews are smoother if staff representatives from both sides are educated on the model. Thus, taking part in formal and informal education on how to use these reviews is strongly encouraged.

2.3.3 General Remarks

The CSIRT Maturity Framework may also be used to audit the maturity level of a (national) CSIRT to provide 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 the Maturity Framework for requirement purposes. For example national CSIRT communities might prescribe the *Basic* or *Intermediate* maturity step as the lowest common denominator and boundary for membership of their community.

3. CONCLUDING REMARKS

The ENISA CSIRT Maturity Framework is a very live concept, which is intensively used by the CSIRTs Network. The national, governmental and sectoral CSIRTs constantly use it to understand, maintain and improve their maturity. The very fact of this active and broad usage means that the Framework needs to be improved regularly.

This report has undertaken that effort for the year of 2021, which also includes new requirements derived from regulatory works, most notably the draft proposal for the EU NIS2 Directive.

The improvement to the framework includes concrete, highly-valuable results – first of all, in the foundation of the framework, the SIM3 standard, where various improvements and updates have been identified in close collaboration with the Open CSIRT Foundation, which maintains SIM3. OCF has agreed to adopt these changes in their forthcoming development of the next version of SIM3.

Another important achievement is that the maturity steps of the ENISA three-tier maturity approach have been brought up to date, also taking into account the proposals for the draft NIS2 Directive.

Finally, the ENISA assessment methodology that consists of self-assessment and peer-review has been extensively improved upon, with a much more detailed approach to the process, including better tooling.

It must be stressed here that the function of this report is to *identify* the aforementioned changes and improvements to the framework, and then to *recommend* them to the CSIRTs Network for implementation.

4. REFERENCES

1. SIM3 standard: https://opencsirt.org/maturity/sim3/
2. FIRST CSIRT Services Framework: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
3. 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 step, this is called 'Advanced' in this document: https://www.enisa.europa.eu/csirts-maturity-sas
4. 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/
5. TF-CSIRT / Trusted Introducer use SIM3 as a basis for the highest tier of their membership, the 'Certified' status: https://www.trusted-introducer.org/processes/certification.html
6. CSIRTs Network, see https://csirtsnetwork.eu/

5. APPENDICES

5.1 APPENDIX A: FAQ

This FAQ section provides informal knowledge about framework-related questions, in order to clarify the framework's context, intent and usage.

Questions on the ENISA CSIRT Maturity Framework

Question: The maturity roadmap has been introduced in this report as a tool to help teams with increasing their maturity in a structured, project-like manner. Will this roadmap also be integrated in SIM3?

Answer: The roadmap is not a SIM3 artefact – SIM3 does not intend to prescribe how to do things, it is a neutral measurement tool. OCF has communicated that this policy will stay the same for SIM3v2. Thus, the roadmap will not be mentioned in any SIM3 parameters. OCF might mention it in accompanying texts like an FAQ of course, as an example of tools to be used to help improve maturity. In this report however, written for CNW/ENISA, the roadmap approach makes perfect sense. The implementation of it is up to CNW/ENISA.

Q: Article 16.2 of the draft proposal for the NIS2 Directive requires a peer review of the CSIRTs' operational capabilities and effectiveness. Is there a risk that there will be two peer reviews, the CNW one, and the NIS2 Directive one?

A: Article 16.2 is indeed a new element compared with the original NISD. It is urgently recommended to the CSIRTs Network and ENISA that they ensure that the next iteration of the CNW peer-review process, for which recommendations are given in this paragraph, are fully aligned with the NIS2 Directive expectations, so as to exclude any double efforts in this area.

Q: The EU Cybersecurity Strategy suggests applying AI in cybersecurity. How is this reflected in the Maturity Framework?

A: For the Maturity Framework, AI usage is implicitly reflected in the SIM3v2i T-8, T-9 and T-10 parameters – the toolsets for incident prevention, detection and resolution. AI is expected to improve the effectiveness and precision of corresponding technologies. In the longer term, one could also expect applications of AI in the Processes category. However, it is expected that for the foreseeable future the human role in CSIRT work will remain crucial, due to the human ability to deal with the unexpected and new, a standard requirement in the CSIRT business.

Q: How does the emergence of the NIS2 Directive affect the Maturity Framework?

A: The latest revised version of the NIS2 Directive proposes more stringent measures for supervision and enforcement, including administrative sanctions, such as fines for breach of the obligations for the management of cybersecurity risk and reporting. Other proposed changes include obligations for the co-ordinated disclosure of newly discovered vulnerabilities across the EU and the streamlined co-ordination of incident reporting with more precise provisions for the reporting process, content and timeline.

For the Maturity Framework, the capability to co-ordinate the disclosure of vulnerabilities and to co-ordinate capabilities in crisis management fall under parameters O-5, P-1 and P-4/5/6/7.

However Article 10 of the Presidency Compromise draft of the NIS2 Directive describes the requirements and tasks of CSIRTs. Some specific relevant parts include the following.

- Article 10.1 (a) focuses on availability of CSIRTs communications services, corresponding with the T-3 and T-5/6/7 parameters.
- Article 10.1 (b) focuses on CSIRTs secure sites (premises and the supporting information systems). This dimension is not explicitly covered in SIM3, but in SIM3v2i it will be added to the description of O-11.
- Article 10.1 (d) focuses on staff resilience, corresponding to the H-2 parameter.
- Article 10.1 (e) focuses on the resilience of systems (redundant systems) and on working space resilience (backup working space). Resilience of systems can be covered partially with the T-3 and T-5/6/7 parameters, but working space resilience is not explicitly covered in SIM3. However in SIM3v2i it will be added to the description of O-11 to include Business Continuity Management

Questions on SIM3 in general

Q: Why is SIM3 not an ISO or IETF standard?

A: OCF has made the conscious decision to not submit SIM3 to any formal standardisation process. The reason for that is that such formal processes, almost without exception, increase the complexity of approaches, certainly over time – and reduce the flexibility. The worldwide success of SIM3 since its introduction in 2008 is based on its simplicity and ease of application. Even with the introduction of SIM3v2 during 2022, which will add some new features and be useful for more types of security teams, the boundary condition of SIM3 will remain very strong: simplicity and ease-of-use. This also keeps the cost of application low.

Questions on the four SIM3 Categories O, H, T and P

Q: It seems that the 17 Process Parameters have rather different natures, from high level to low level. Is the word 'process' really warranted for all of them?

A: This was a deliberate determination in the design of SIM3, to avoid excessive complexity. In fact, there are potentially three Ps in the 'P' category: policies, processes and procedures. They have, for the sake of convenience, all been listed under the Processes category but they indeed have different natures.

Q: Why are O-6 (Public Media Policy) and O-11 (Security Policy) not in the Processes category, as you could argue these are really more akin to the kind of parameters found in that Category?

A: The reason they are in the Organisation Category is that O-6 and O-11 are both quite fundamental policies that are an essential part of the organisational make-up of CSIRTs. This is why it was decided to have them in the 'O' Category.

Questions on the SIM3 levels 0 to 4 and related evidence gathering

Q: How can I figure out if the parameter is level 3 or 4?

A: Essentially, the parameter is level 4 when there is regular checking, assessing or auditing of this parameter on the authority above team manager and a feedback mechanism is preserved throughout.

This is intended to ensure that the higher level of governance is actively aware of some of the crucial aspects of the CSIRT and how it functions in real life.

Q: Our team manager conducts an internal compliance review every year for our own purposes. SIM3 methodology is used as a framework in the review. Does that count for level 4?

A: No, because the process lacks involvement of the higher governance.

Q: Our team manager sends a report to higher governance every year, and the report explicitly refers to seven of the SIM3 parameters. Does that mean those parameters can go to level 4?

A: No, because sending a report to higher governance does not satisfy the level 4 requirements; a regular audit or review needs to be done on the authority of higher governance, and there needs to be a feedback loop with the team, aiming for improvements. Just sending a report really means nothing as yet, therefore this does not warrant level 4 in any way.

Q: Our management board commissions an audit of our unit to the internal audit unit. This is a part of an annual [PUT ANY STANDARD HERE] compliance review. The audit report is presented to the management board along with findings and recommended actions. The annual review also pertains to the actions taken by the team since the previous audit. Does that count for level 4?

A: Yes, but only when it is explicit enough in mentioning the aspects corresponding with SIM3 parameters. It will probably also only work towards a subset of the SIM3 Parameters, since SIM3 does not fully map to any of the known formal standards. Thus, it is strongly recommended to use SIM3 as one of the controlling documents in such audits.

Q: The topic of a parameter is covered in our cybersecurity legislation. Is this sufficient for level 4?

A: Yes, but only when the law mentions it explicitly – and when the function is indeed implemented within the team. Thus, this still requires documentation inside the team for such aspects and embedding it in a team information system, processes, service description etc.

Q: How can I know if evidence is suitable for a particular parameter?

A: Due to the specific characteristics of each team, the SIM3 methodology tries not to indicate a specific set of evidence for achieving a specific level of maturity. Therefore, a predetermined closed checklist for the parameter (and the maturity level assigned) cannot be introduced. Additionally, in terms of finding evidence and assessing its relevance, SIM3 does not require a special approach.

There are some good practices (apart from common sense!) that can be conducted to ease this process. The person who performs the self-assessment may do the following.

1. Identify all relevant parties to the CSIRT functions (e.g. CISO, CIO, BCM Unit, IT Department, Legal Office, Communication Department, HR, Internal Audit) simply in order to ask for a particular piece of information or document.
2. Collect all physical and electronic documentation. This may include procedures, instructions, playbooks, policies, regulatory documents, control lists, incident response plans, contact lists, diagrams, etc. These may already be collected for the purposes of another assessment.
3. If applicable, look for documents scoped by the integrated management systems (usually the Information Security Management System is relevant here).
4. If applicable, look for any previous reports from security audits.

5. Identify all knowledge bases that are used within the CSIRT – these may be sources such as an internal wiki and intranet.
6. Create a list of the most important technologies and tools that are used by CSIRTs. Identify what they are used for and who uses and manages them.

Q: What is the optimal level to which we should strive while building the maturity of the team? Our management usually requires us to achieve the highest scores in this type of assessment.

A: It should have been emphasised that it is not necessary or required to 'push' everything to level 4 unless it comes naturally from continuous improvement. The OCF SIM3 standard scoring should not be treated as a linear solution. SIM3 does not require a CSIRT to implement an elementary approach in which the only strategy should be to reach the highest possible score for every parameter. The scoring system from 0 to 4 is only the probe of technical interpretation of the controlled area. The real need for achieving a particular level of the maturity bases depends on many factors such as a strategy, a mission, priorities, operational needs etc. Thus, the strategy for the development of a national level CSIRT differs much from a CSIRT strategy of a small or medium-sized organisation. The roadmap to the maturity of any CSIRT should be determined individually or based on some recommendation (e.g. TF-CSIRT Trusted Introduction certification schema or ENISA/GCMG profiles). A consciously-developed strategy can positively influence the conduct of an optimal long-term development of CSIRT maturity.

Q: The potentially-long process of developing an assessment report prevents us from taking action. Is there any template or tools that we can use to speed up the process?

The following two (optional) documents have been made available to help the assessment and peer-review process:

1. CSIRT maturity evaluation report template (see Appendix C)
2. CSIRT maturity evaluation spreadsheet (see Appendix D)

Both documents can be used together for the purpose of self-assessment and peer-review, in conjunction with ENISA's online maturity self-assessment tool.

Questions on the SIM3 parameters

Q: What is the difference between O-3 and O-4?

A: O-3 is the authority of the team – what it is allowed to do towards its constituency, based on its mandate (O-1) – the power of the team. Is that power just advisory? Or can the team also escalate? Or can it also enforce (e.g. port filtering, blocking, etc.)? Clearly, the authority of the team needs to come from higher governance or else there will be no high-level support for the team in cases where the power needs to be used.

O-4 is the responsibility of the team – what it is expected to do towards their constituency, again based on its mandate. Basically, the responsibility is a high-level version of what is detailed in the team's services (O-5). In almost all cases, a team has more responsibility than authority. For example: a team may well be responsible for checking out if new threats could hurt their constituency, e.g. by doing non-interruptive port scans. But that is not to say that the team has the authority to go beyond 'non-interruptive' scans or that, if the team finds such vulnerabilities, it can give orders to the constituents in question; this will often be in the form of advice, not enforcement.

A situation to avoid is where a team's authority is very small but their responsibility very big. If the gap between O-3 and O-4 becomes too great then a team is more or less expected to do

many things without having the power to actually make them work. That is a recipe for malfunctioning. There is a natural gap between O-3 and O-4 but it should not become too wide.

Q: Why does P-8 combine audit and feedback? Why not treat them separately?

A: The essential idea behind P-8 is that it should help teams to foster a fruitful collaboration between a team's higher governance level(s) and the team itself. This is also the essence of maturity level 4. Collaboration only exists by virtue of two-way communication. The mechanism chosen in P-8 to support and inspire this is the method of 'audit' on the authority of higher governance. But such an audit is only useful when followed by feedback to the team. The goal is that the audit (or review or assessment) leads to a fruitful communication (feedback) between the higher governance and the team – which then should lead to whatever changes or improvements are needed, such as hiring more people, or more specialised people; sending team members for specific training; increasing the tooling of the team; optimising various processes; improving the outreach of the team; etc.

Q: Can P-8 help to bring parameters to level 4?

A: Yes, that is one of the design functions of P-8. When the P-8 process or policy is specific enough, it can lead to parameters being rated at level 4. What is needed is simple enough. When P-8 specifically refers to certain aspects, corresponding to specific parameters, and the policy ensures that:

1. the audit (or review or assessment) is done on the authority of the higher governance level(s);
2. the audit is done regularly (typically once or twice a year – once every two years is seen as the minimum); and
3. there is feedback after the audit to the team in order to establish two-way communication between the team and higher governance, with the aim of improving the team's set-up and operations;

then such parameters can be rated at level 4.

Of course, when all this is the case and such audits have already been performed then the obvious request of any external auditor (or peer-reviewer) will be to examine one of the audit reports, and the consequences arising therefrom – and the team needs to be prepared to oblige.

Q: What kind of 'audit' is meant in P-8? Formal or informal, internal or external, etc.?

A: The audits meant in P-8 are really any type of audit, review or assessment. If a team does internal evaluations twice a year, this can be listed under P-8 and the question is then simply whether it is level 2, 3 or 4 (level 1 seems unlikely, as such audits are rarely documented). Indeed, internal evaluations can be at level 4 provided level 4 requirements are met, which would mean that such an evaluation scheme would need to be approved by higher governance and checked regularly. However, an internal evaluation only by the team will never make it possible to lift parameters other than P-8 itself to level 4 because, for example, even if that evaluation explicitly includes O-1 and O-5 every year, it does not satisfy the level 4 demands for O-1 and O-5, and so O-1 and O-5 cannot be raised to level 4.

Thus, to use P-8 as enabler for level 4 (see the previous Q&A) it is necessary that there is also a regular audit or evaluation on the authority of higher governance, including a feedback loop to the team – and that it is made explicit what such an audit will (at least) cover.

Q: The updated Maturity Evaluation Spreadsheet contains an 'Evidence collected' column. What information should we add to this column?

A: The information about the evidence should refer to the type of evidence (document, screenshot, part of an internal wiki etc.) and the name or, if the evidence has no name, a brief

description of what it is about. Excerpts from evidence placed in cells are not required. Evidence names should be consistent for all parameters.

5.2 APPENDIX B: COMMENTS ON ALIGNMENT TO CYBERSECURITY STRATEGY AND NIS2 DIRECTIVE

New EU Cybersecurity Strategy

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy for the Digital Decade. The EU's new Cybersecurity Strategy aims to ensure a global and open Internet with strong guardrails to address the risks to the security and fundamental rights and freedoms of people in Europe. Following the progress achieved under the previous strategies, the strategy contains concrete proposals for deploying three principal instruments – regulatory, investment and policy – to address three areas of EU action:

(1) resilience, technological sovereignty and leadership,
(2) building operational capacity to prevent, deter and respond, and
(3) advancing a global and open cyberspace.

Some of initiatives will have an impact on how national, sectorial or private CSIRTs and SOCs should operate – for example, the initiative to build a European Cyber Shield; the Commission proposes to build a network of Security Operations Centres across the EU. Effective collaboration of SOCs from different types of organisations and nations will be possible just by building mutual understanding and trust between the teams.

Recommendations for future framework development:

1. A specific maturity profile might be useful to indicate whether the maturity level of a SOC is sufficient for it to be accepted into the 'EU's Cyber Shield' network. To be analysed in future work.

Additionally, the question of the use of AI is addressed in FAQ section.

Proposal for NIS Directive

The Directive on Security of Network and Information Systems (the NIS Directive) provides legal measures to boost the overall level of cybersecurity in the EU. It came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation of the last years, the time has come to refresh it. The revised Directive was proposed on 16 December 2020.

The revised version proposes more stringent measures for supervision and enforcement, including administrative sanctions, such as fines for breaches of the obligations to manage and report cybersecurity risk. Other changes propose increased information sharing and co-operation between authorities in Member States with the enhanced role of the Co-operation Group; co-ordinated disclosure of newly discovered vulnerabilities across the EU; streamlined obligations to report incidents with more precise provisions on the reporting process, content and timeline; as well as an expanded scope to include more sectors and services as either essential or important entities.

It is additionally addressed in the FAQ section.

5.3 APPENDIX C: UPDATE OF THREE-TIER MATURITY APPROACH AND SIM3 STANDARD

The table below presents the minimum scores required for the three steps of maturity, similar to Table 3 in Chapter 3, but the version here also highlights the changes between the old ENISA Framework and the current one – and thus also the most significant changes between SIM3v1 and SIM3v2i. In addition, it indicates what increases in the overall requirements for maturity in the three steps.

Parameter number	Parameter Description	Minimum values for the tiers:		
		Basic	Intermediate	Advanced
O-1	Mandate	3	4	4
O-2	Constituency	3	4	4
O-3	Authority	3	4	4
	In the description in SIM3v2i it will be explicitly stated that the whole purpose of the O-3 parameter is to help ensure that a CSIRT has a clear and distinct description of its authority. If the cyber security law can provide that clarity for an nCSIRT, so much the better – if the law is not very specific then the CSIRT should make sure that the authority is defined more precisely, starting from the law. Also the difference between O-3 and O-4 will be explained better (also see FAQ).			
O-4	Responsibility	3	4	4
	In the description in SIM3v2i the difference between O-3 and O-4 will be explained better (see also FAQ).			
O-5	Service Description	3	4	4
	In the description in SIM3v2i it will be stated explicitly that the concept of O-5 and O-7 is only to ask 'have you defined your services towards the constituency (O-5) and the service levels thereof (O-7)?' Detailing what those services should or should not be is up to the team as SIM3 makes no specific requirements on these matters – although, of course, in other parameters it is assumed that every CSIRT at least deals with Incident Management as a service. It will also be stated that SIM3 serves as the overall maturity standard for the CSIRT, and can be visualised by a horizontal line with the forty-five parameters as ticks on that line. On O-5 (and O-7) a vertical line intersects the SIM3 horizontal line; that vertical line is the visualisation of the FIRST CSIRT Services Framework, which every team is strongly recommended to use to map their services portfolio in detail.			
O-6	N/a > Public Media Policy	- > 2	- > 3	- > 4
	O-6 has been added as a new parameter in SIM3v2i in the space that in SIM3v1 was 'intentionally left blank'. O-6 is about how to work together with the press and how to conduct public communications in general. The NIS2 Directive makes it necessary to aim high here, starting with a minimum of level 2 and growing towards level 4. This is aligned with the demands for O-11 (identical) and P-2 (the same for Basic and Intermediate but, for Advanced, level 4 is requested for O-6 policy whereas for the P-2 process, level 3 is regarded as sufficient).			
O-7	Service Level Description	3	3 > 4	3 > 4
	The levels here are aligned with O-5. In general, the move from NISD to the NIS2 Directive comes with higher service demands, which makes this alignment logical. The 1.5 year re-assessment time-interval should allow sufficient time for this change.			
O-8	Incident Classification	1 > 2	2 > 3	3

	The ENISA supported 'common taxonomy' will be referred to explicitly in SIM3v2i. Based on the NIS2 Directive it is reasonable to demand at least level 2 for Basic, growing to level 3 for Intermediate, while Advanced can stay on level 3.			
O-9	Integration with existing CSIRT Systems > Participation in CSIRT Systems	3	4	4
	The name change for the parameter is a straightforward improvement, leaving out the superfluous word 'existing' (one can only participate in a system if it exists), and changing 'integration' into 'participation' as that better reflects the reality. It will be explicitly emphasised how important the participation in national CSIRT networks is also, apart from regional ones (such as CNW and TF-CSIRT), and global ones. Where the focus of participation will be depends on the type of team.			
O-10	Organisational Framework	3	3	3
	In the description in SIM3v2i it will be stressed that O-10 does not have to be one single document. It will also be stated that RFC 2350 can be part of O-10 but not all of it, and that RFC 2350 is essentially a public document, whereas O-10 is an internal controlling document, often referred to as the 'team charter'. For CSIRTs, most of O-10 can be in the law – yet even then it can be very useful to re-iterate the O-10-related aspects in, for example, a team wiki, with the correct references. It will also be stressed that the great use of having a consolidated write-up of O-10 (even if it is more than one document) is that this is indeed the high-level 'charter' of any team – the controlling document describing who and what they are, and what is expected of them. This is the kind of controlling document for which the approval of higher governance is needed, and can then serve as a reference for the functioning of the team, for audits etc.			
O-11	Security Policy	1 > 2	2 > 3	3 > 4
	In the description in SIM3v2i or FAQ, that business continuity (and BCM) is an essential element of information security will be added – references will also be made to the resilience' of T parameters and to H-2. Given the NIS2 Directive and the importance of business continuity, the level of demands here have been upgraded by +1 for all three tiers, leading to level 4 at the Advanced tier. Additionally the NIS2 Directive (Article 10.1.(b) and €) has expectations in this area, that they align with the levels here – more specifically, the NIS2 Directive asks for secure sites (premises and the supporting information systems) and for working space resilience (backup working space). SIM3 is a global standard and therefore does not reflect any specific national or regional situation. However the concept of site and workspace resilience will be added explicitly to the BCM aspect of O-11 in SIM3v2i.			
*O-**	*maturity increase (O-6 not counted)*	*+2*	*+3*	*+2*
H-1	Code of Conduct/Practice/Ethics	2	3	3
	SIM3v2i or FAQ emphasise that a generic ethics code is good, but has nothing to do with CSIRT work – therefore make sure to have your own ethics code. Highlight both CCoP and EthicsFIRST and suggest that specific CSIRT co-operatives can create their own ethics code.			
H-2	Personnel Resilience > Staff Resilience	2	3	3 > 4
	The parameter name change is done to (a) avoid the previous confusion between 'personal' and 'personnel' and (b) to align with the use of 'staff' in H-4. As O-11 is improved to explicitly include business continuity, H-2 is related, as 'having enough people on the job' is a boundary condition for BCM. The level demands for both have been aligned – a level 4 for Advanced is clearly necessary for H-2. Additionally, the NIS2 Directive (Article 10.1.(d)) has expectations in this area – that there is alignment with the levels here.			

H-3	Skillset Description	1 > 2	2	3
	Even at the Basic step, a written skillset description is needed when hiring professionals, hence level 2. The forthcoming FIRST role/skillset document can be used as a reference.			
H-4	Internal Training > Staff Development	1 > 2	2 > 3	3 > 4
	SIM3v2i clarifies that this parameter is about staff development as a whole, thus the name change, including personal development plans, and team building or education – much of it will be 'internal' but not necessarily so. H-5 and H-6 zoom in on two important aspects thereof, important enough to warrant separate parameters, but H-4 is the high-level aspect. nCSIRTs are high-profile teams paid for by public money – therefore the Advanced step needs to be at level 4, with proper auditing and feedback. The Basic step already needs to be level 2, just as H-3 is at level 2 for Basic – the H-4 programme leans on H-3 skillsets for roles.			
H-5	External Technical Training > Technical Training	1	2	3
	SIM3v2i clarifies that H-5 is a specific, crucial part of the H-4 programme, requiring hard budgets and prioritisation. It does not have to be 'external,' hence that is left out. Also added in SIM3v2i or the FAQ is that it is about hard skills in general, as opposed to the soft skills that are the topic of H-6.			
H-6	(External) Communication Training > Soft Skills Training	1	2	3
	SIM3v2i clarifies that H-6 is a specific, crucial part of the H-4 programme, requiring hard budgets and prioritisation. It does not have to be 'external', hence that is omitted. It is also generalised to say 'soft skills' complement the 'hard skills' from H-5. SIM3v2i or FAQ also add that the soft skills include the essential topics of human communication (and not just talking with the press – it is a skill that's needed by CSIRT members in general), team building, working under stress, etc.			
H-7	External Networking	2	3	3
*H-**	*maturity increase*	*+2*	*+1*	*+2*
T-1	IT Resources List > IT Assets & Configurations	1	1 > 2	1 > 3
	SIM3v2i clarifies that 'assets' is a more meaningful name than 'resources' and that T-1 is about more than just those assets – it is about knowing, to some reasonable extent, what the constituents have in terms of hardware, firmware and software, and how it is configured. 'Assets & Configurations' seems, as a whole, to describe that well. With increasing emphasis on CIIP, it is not acceptable to have level 1 across the board here – a growth to level 3 for Advanced is entirely warranted. An nCSIRT may not have to know all details of assets and configurations but, to some degree, there must be sufficient knowledge of the main systems and software in use inside the CIIP, or else it is impossible to do targeted threat intel and provide targeted advice.			
T-2	Information Sources List	1 > 2	2 > 3	3 > 4
	The NIS2 Directive specifically mentions Vulnerability Management, thus upping the ante for T-2 and P-12. Level 2 is thus the minimum to start with for Basic, growing to level 4 for Advanced. Level 2 means that an informal list (e.g. on a team wiki) can be maintained, which is very easy and really the minimum needed. For Intermediate, this list can still be on, for example, the team wiki, but its existence *and maintenance* needs to have approval from the team management. Level 3 does not mean the list has to become static, it can still be dynamic, as long as the *process* (see also P-12) for approval (and removal) of information sources has management support. Level 4 for Advanced means that this list and its maintenance are subject to audit and feedback by higher governance.			

T-3	Consolidated E-Mail System > Consolidated Messaging System(s)	1 > 2	2 > 3	3
	SIM3v2i clarifies the name change based on the fact that 'messaging' nowadays is a more generic name for e-mail and other messaging systems (signal, threema et al.) that are in use concurrently for similar purposes. These need to be consolidated one way or another. As to levels, by definition, a functioning messaging system is already at level 2 (Basic) and a growth to level 3 (Intermediate) already is logical, as this important parameter requires management oversight and approval. Additionally the NIS2 Directive (Article 10.1.(a) and (e)) has expectations in this area that align with the levels here.			
T-4	Incident Tracking System	1 > 2	2 > 3	3
	No name change needed, but otherwise similar reasoning for level changes as with T-3.			
T-5	Resilient Phone > Resilient Voice Calls	1 > 2	2 > 3	3
	SIM3v2i replaces 'phone' by 'voice calls'. It clarifies that the old mechanism of real-time voice or phone calls is as important as it always was, which also applies to CSIRT work. In some cases we can conveniently add video calls to that, creating another dimension. The demands for levels have been synchronised with those for H-2 – as this is all about business continuity. Therefore starting at Basic with level 2 is necessary – but whilst growing to level 4 is necessary for H-2, it is sufficient to stop at level 3 for T-5 to T-7, as it is enough that these are managed on the level of the CSIRT; they do not require a higher governance audit. Additionally, the NIS2 Directive (Article 10.1.(a) and (e)) has expectations in this area that align with the levels here.			
T-6	Resilient E-Mail > Resilient Messaging	1 > 2	2 > 3	3
	Like for T-3, updating the name from 'e-mail' to 'messaging'. The changes in levels here follow the exact same logic as described for T-5. Additionally, the NIS2 Directive (Article 10.1 (a) and (e)) has expectations in this area that align with the levels here.			
T-7	Resilient Internet Access	1 > 2	2 > 3	3
	The changes in levels here follow the exact same logic as described for T-5. Additionally, the NIS2 Directive (Article 10.1.(a) and (e)) has expectations in this area that align with the levels here.			
T-8	Incident Prevention Toolset	1 > 2	1 > 2	1 > 3
	A description on, for example, a wiki (level 2) is regarded as the absolute minimum for T-8 to T-10, in order that all team members can know and access the relevant tools – this is generally enough for T-8. However the NIS2 Directive is explicit about prevention activities (such as vulnerability management) and therefore a level 3 for Advanced is necessary.			
T-9	Incident Detection Toolset	1 > 2	1 > 3	1 > 3
	As for T-8, a description on, for example, a wiki (level 2) is regarded as the absolute minimum here. However given the crucial significance for CSIRTs of incident detection and resolution, also explicated in the NIS2 Directive, level 3 is warranted for both Intermediate and Advanced. For the associated process, the demand for Advanced will even be level 4.			
T-10	Incident Resolution Toolset	1 > 2	1 > 3	2 > 3
	As for T-8, a description on, for example, a wiki (level 2) is regarded as the absolute minimum here. However given the crucial significance for CSIRTs of incident detection and resolution, also explicated in NIS2 Directive, level 3 is warranted for both Intermediate and Advanced. For the associated process, the demand for Advanced will even be level 4.			

*T-**	*maturity increase*	*+9*	*+12*	*+8*
P-1	Escalation to Governance Level	3	3 > 4	3 > 4
	Levels are aligned with those for the parameters O-1 to O-5, as this escalation is equally crucial.			
P-2	Escalation to Press Function	1 > 2	2 > 3	3
	This important escalation needs to be approved by the CSIRT manager when it is at least already at the Intermediate level. Levels are synchronised with the new P-6 parameter. Advanced level 3 is seen as sufficient here, while the press policy O-6 itself needs level 4 for Advanced.			
P-3	Escalation to Legal Function	1 > 2	2 > 3	3
	Same levels and reasoning as for P-2.			
P-4	Incident Prevention Process	1 > 2	2 > 3	2 > 4
	Levels follow the same reasoning as for the associated T-8. However for Advanced, level 4 is required, as the importance of this process under the NIS2 Directive warrants auditing & feedback.			
P-5	Incident Detection Process	1 > 2	2 > 3	2 > 4
	Levels follow the same reasoning as for the associated T-9. However for Advanced, level 4 is required, as the importance of this process under the NIS2 Directive warrants auditing & feedback.			
P-6	Incident Resolution Process	1 > 2	2 > 3	2 > 4
	Levels follow the same reasoning as for the associated T-10. However for Advanced, level 4 is required, as the importance of this process under the NIS2 Directive warrants auditing & feedback.			
P-7	Specific Incident Processes	1 > 2	2 > 3	2 > 4
	Levels follow the same reasoning as for P-5 and 6.			
P-8	Audit/Feedback Process > Audit & Feedback Process	2 > 3	3 > 4	4
	SIM3v2i and the FAQ add the aspect(s) of innovation, agility and flexibility to P-8 – how fast the CSIRT invents and builds new tools and services according to new technology and legal changes, i.e. the capability to adapt, generally speaking. You should also stress that this is about audit *and* feedback from higher governance to the team – hence the slight name change – explaining the idea of audit *and* feedback thoroughly to avoid confusion. Explain that in general it is a good idea to explicitly refer in P-8 to those parameters that need to be at level 4. Levels must be aligned with O-1 to O-5.			
P-9	Emergency Reachability Process	2	3	3
P-10	Best Practice E-mail and Web Presence > Best Practice Internet Presence	2	2 > 3	2 > 3
	In SIM3v2i the name change is explained – it is especially due to the fact that social media have become important parts of the team's online presence. Also, the new description will be more explanatory, less prescriptive, similar to P-13. It is about having a clear process to deal with the team's presence on the Internet, rather than with the detailed implementation thereof. The changes in level are due to the fact that it is essential in an early stage that team management approves the team's Internet presence; hence level 3 for Intermediate and Advanced.			
P-11	Secure Information Handling Process	2	3	3
	SIM3v2i will additionally state that P-11 should incorporate compliance with applicable privacy laws, such as the GDPR and others, depending on where the team is based. The NIS2 Directive (Recital 69 and 70) has expectations in the area of GDPR that align with the levels here.			
P-12	Information Sources Process	1 > 2	2 > 3	3 > 4

	Levels change based on same reasoning as for T-2, NISDS2 increased priority.			
P-13	Outreach Process	1 > 2	2 > 3	3 > 4
	SIM3v2i or the FAQ clarify that this process should be two-way – it should include modes of feedback from constituency to team. This is different from the feedback in P-8, which is from higher governance. Level-wise, the NIS2 Directive warrants level 4 for Advanced, and any outreach to the constituency really cannot be level 1, thus making level 2 the minim for Basic.			
P-14	Reporting Process > Governance Reporting Process	2 > 3	3 > 4	4
	SIM3v2i explains the name change as follows: as P-14 and P-15 are now both about reporting processes, the difference between them needs to be made clear. Level-wise, it is aligned with O-1 to O-5, and the NIS2 Directive requires that along with an emphasis on (mandatory) reporting.			
P-15	Statistics Process > Constituency Reporting Process	1 > 2	2 > 3	3
	SIM3v2i makes clear that this parameter was and is really about what and how you report to your constituency, as opposed to your governance (P-14) – whether that includes statistics or not is less relevant, hence the name change. Level wise this is sensitive enough to require a minimum of level 2 for Basic – whereas management approval is needed the sooner the better, hence twice level 3. In the tooling, level 1 could be present for P-15, but choosing level 1 does not allow P-15 to be disregarded, as level 1 is not a valid option for Basic, Intermediate and Advanced steps, and that should show in the tool. It is a valid option for the Under-basic step however.			
P-16	Meeting Process	1 > 2	1 > 2	2 > 3
	SIM3v2i or the FAQ has added online and hybrid meetings as options. Level-wise, this parameter is so important (and some degree of notes taking must be in place) that level 2 is seen as the absolute minimum. Level 3 is sufficient and required for Advanced.			
P-17	Peer-to-Peer Process > Peer Collaboration Process	1 > 2	1 > 3	2 > 4
	In SIM3v2i the name change is clarified, and also that this parameter is about working together with other security teams (CSIRTs, SOCs, PSIRTs etc.) outside but also inside the constituency. Again, the feedback from (in this case) peers should be part of the process, like in P-8 (feedback from higher governance) and P-13 (feedback from the constituency). Information sharing is an explicit topic in the NIS2 Directive, thus a level upgrade is warranted to start with level 2 for Basic and go towards level 4 for Advanced.			
*P-**	*maturity increase*	*+13*	*+16*	*+15*

TP-07-22-077-EN-N X

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high, common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, co-operates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-563-0
doi: 10.2824/35453