CERT community

Recognition mechanisms and schemes

November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

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

Authors

Andrea Dufková – ENISA (main editor)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.

For media enquiries about this document please use press@enisa.europa.eu.

Acknowledgements

The analysis in this document was produced in collaboration with a team from IDC CEMA: (Joshua Budd, Jachym Homola and Matthew Marden).

We would like to thank all the CERTs that participated in the survey conducted to provide input into this document: FIRST education committee, European n/g CERTs as well as the TF-CSIRT community.

ISBN 978-92-79-00077-5 doi:10.2788/14231

Executive summary

This document provides an **overview of existing mechanisms supporting Computer Emergency Response Teams (CERTs)** to deploy capabilities necessary for their operations and their maturity level. It introduces these mechanisms according to the CERT maturity levels that they address based on **eight predefined criteria** including requirements that CERTs must meet; CERTs' focus: type or region; and definitions and terminology used.

A three-tier CERT maturity model was specifically developed for the purpose of this project, with the tiers being three respective stages of a CERT development: fundamental, baseline and advanced. At each stage of this progression, mechanisms from CERT community organisations provide guidance and support to CERTs with regard to the defined categories.

For all three tiers the document highlights important **commonalities and differences among the mechanisms**. This enables the **identification of potential areas for harmonisation** of the CERT mechanisms, though this document does not aspire to determine how, when or by whom the harmonisation efforts should be carried out.

As partly confirmed by direct consultations with them while preparing this paper, CERTs are in need of harmonisation for the following reasons:

- **Requirements and validation process**: CERTs need to meet and adhere to different requirements, which is resource- and time-intensive. This would be much more effective and easier based on harmonisation across the CERT community.
- **Definitions and terminology:** Many terms and definitions used by CERT organisations are already similar. Harmonising core terms such as CERT (CSIRT), constituency, or incident would make these mechanisms significantly more compatible and make it easier for CERTs to subscribe to, or utilise, various mechanisms.
- **CERT types (sectors)**: It could be beneficial for different mechanisms to harmonise their definitions of sectors that vertical-specific CERTs typically focus on, and to specify clearly various constituency types, as doing so would offer more clarity and transparency surrounding CERT activities.
- **Training:** Harmonisation could lead to synergies, proliferation of training opportunities for CERTs, and more opportunities for CERTs to meet and share good practices. Good progress has already taken place in this respect with several CERT organisations including ENISA and FIRST supporting TERENA's TRANSITS training for CERTs, and ENISA producing material that actively is rolled out to CERTs on request.

Table of Contents

1 Introduction

1.1 Aim and scope of the document

In the context of this document the term “mechanism” refers either to the description of CERT capabilities (WHAT) for a certain maturity level (e.g. baseline capabilities for n/g CERT mechanism of ENISA[1]) or to the procedure (HOW), which is used to get to a certain maturity level (e.g. accreditation mechanism of Trusted Introducer[2]). Term “scheme” is used as a synonym to the term “mechanism” in this regard.

There exist several mechanisms that support CERTs and their common processes. They can describe how to set up the CERT and its daily life; the services teams provide; or the way they cooperate. These CERT mechanisms vary depending on the maturity level of the CERTs concerned.

In this document we first provide an overview of the organisations behind these mechanisms and the sort of criteria used to describe the maturity level of a CERT (section 2). Then we present a three-tier model of CERTs’ maturity specifically developed for this project (section 3), with the respective tiers Fundamental, Baseline and Advanced. The individual CERT mechanisms of various CERT organisations are attached to these respective tiers. In section 4 we identify the commonalities and differences among the mechanisms within the three maturity tiers. In section 5 we provide some recommendations for areas considered suitable for harmonisation efforts.

It should be stressed here that the document does not aim to provide any kind of rating of the mechanisms, but rather to show what is currently in use by CERTs and which areas of these mechanisms could be improved (harmonised).

1.2 Methodology

Extensive desk research was conducted to prepare this document, using mostly publicly available sources linked to CERT mechanisms, CERT organisations and CERT communities. The sources are always referenced in the text. A concise survey was also launched to gather stakeholders’ views on the need for harmonisation of CERT schemes. Sixteen teams, mostly national/ governmental CERTs, provided replies to the survey. The survey focused on the capabilities schemes followed by CERTs, the need to harmonise these them and identify new areas for harmonisation.

[1] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities
[2] https://www.trusted-introducer.org/processes/accreditation.html

2 How do you assess a CERT's maturity?

A number of organisations,[3] both in Europe and internationally, provide different mechanisms for supporting and advancing CERT capabilities and therefore their maturity. These CERT community organisations provide useful insights into the operations of CERTs and their cooperative efforts, as well as the policies, procedures and tools used by different teams. As CERTs continue to develop their capabilities and become more accepted by their constituents, they also cooperate more often with other CERTs both in their home countries and internationally and look to gain recognition from more partners. The maturation of CERTs and their use of different CERT mechanisms mean that there is a greater need to explore whether harmonisation between them may be beneficial, and which areas could potentially be harmonised.

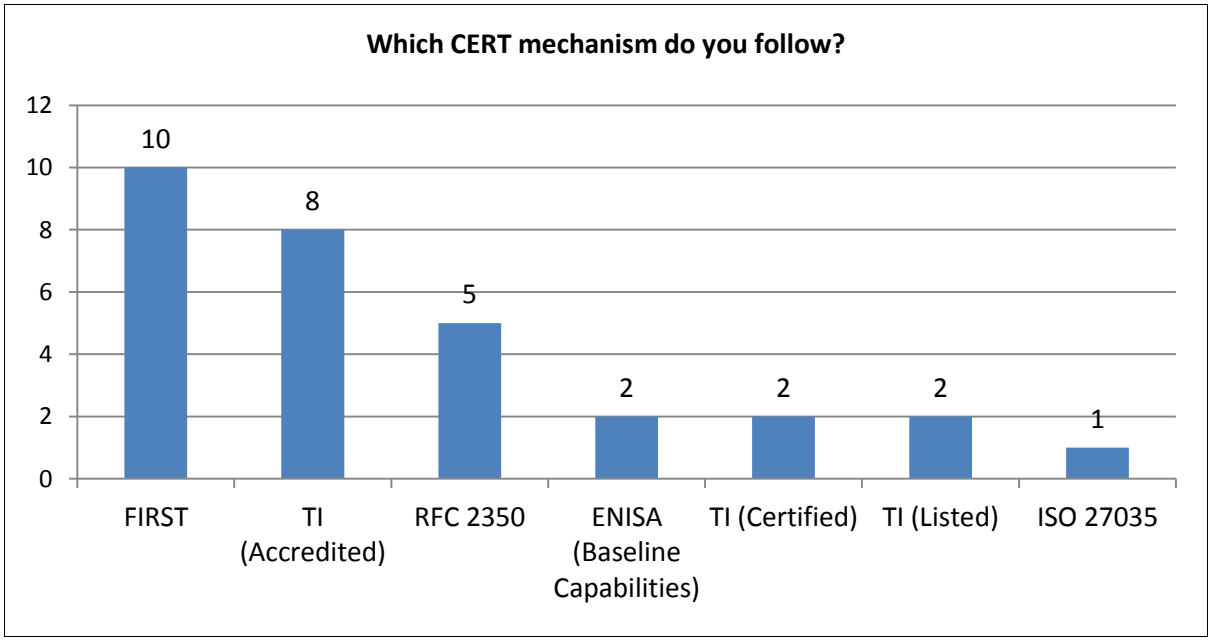
This section of the report provides an overview of a number of mechanisms used frequently by CERTs, which deal with and consider CERT capabilities. The mechanisms that have been introduced vary in their objectives and means of achieving these objectives, and are thus used in different ways by CERTs.

2.1 Which organisations support CERTs and promote their maturity?

CERTs can look to a number of organisations for suitable mechanisms and good practices. These mechanisms range from being global in scope (e.g. FIRST) to regional (e.g. APCERT) or to more service-specific oriented (e.g. ISO 27035). As discussed later in this report, these organisations provide mechanisms and good practices for CERTs at various points in the CERT maturation process.

ENISA surveyed the European CERT community and asked them which mechanisms they follow. Many of the respondents report following several different CERT capabilities mechanisms, with Trusted Introducer (TI) and FIRST being named most often.

[3] *As used in this document, the term 'organisation' or 'CERT-type organisation', means any type of organisation, association, gathering or institution whose aim is to provide a platform of cooperation among CERTs and/or provide standards, guidance or good practices for their activities.*



Number of answers =16 (respondents had the option to choose more than one scheme)

Source: Survey conducted by ENISA to provide input into this document

2.1.1 ENISA

ENISA was established in 2004 to improve network and information security in the European Union (EU). It was intended to be the EU's response to the emergence of cyber-security as a significant issue impacting EU Member States and businesses. ENISA serves both EU institutions and Member States, including public and private organisations.

In June 2013, the EU granted ENISA a further seven-year mandate with an expanded set of duties.[4] In addition to enshrining ENISA's achievements in areas such as helping EU Member States set up CERTs and provide cyber-security exercises, the new mandate:

- Provides ENISA with instruments to support the fight against cybercrime based on prevention and detection in cooperation with Europol's European Cybercrime Center;
- Gives ENISA responsibility for supporting the development of EU cyber-security policy and legislation;
- Looks to ENISA to support research, development, and standardisation;
- Charges ENISA with supporting the prevention, detection of, and response to cross-border cyber-threats; and
- Aligns ENISA more closely with the EU regulatory process for providing EU countries and institutions with assistance and advice on cyber-security issues.

ENISA describes its role with regard to CERTs in Europe as a facilitator and information knowledge broker rather than having an operational role. As the EU 'expert body' on CERTs, ENISA must remain updated about key issues impacting CERTs, and establish and maintain contacts with important global players in the CERT field, including those profiled in this report. ENISA also distributes good

[4] Regulation (EU) No. 526/2013, available at http://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties

practices to CERTs within its purview, and helps to organise and host workshops and other events and conferences for them.

One of ENISA's priorities is to help EU Member States establish national/ governmental (n/g) CERTs and support these teams' efforts to reach a baseline level of capabilities as they mature. In addition to the baseline mechanism, ENISA further supports CERTs' efforts to enhance their capabilities by providing, for example, tailored training.

ENISA originally published baseline capabilities documents for CERTs in 2009. The technical aspects of these reports were extended by policy recommendations to n/g CERTs in 2010[5] as to the four baseline capabilities that they should have. The latest update of the baseline capabilities recommendations was completed in 2012.[6]

ENISA also regularly publishes a CERT Inventory map and an *Inventory of CERT Activities in Europe* document. Both are updated twice a year and largely correspond to the Trusted Introducer database of listed teams.[7]

In 2013 ENISA introduced its training courses for CERTs in the EU Member States. This is a new initiative to promote and support CERT maturity in the MS by having exercises and technical hands-on training on different services, operations and cooperation in daily work of the teams.[8]

2.1.2 TF-CSIRT Trusted Introducer

TF-CSIRT Trusted Introducer (TF-CSIRT/TI)[9] is the new name for the integrated TF-CSIRT and Trusted Introducer operations under the Trans-European Research and Education Networking Association (TERENA[10]) structure. It is an example of a CERT membership organisation that focuses on a particular region. The Task Force for Computer Security Incident Response Teams (TF-CSIRT) was established in 2000 and has evolved into a much-used forum by various CERTs for discussion of experiences and knowledge. The Trusted Introducer (TI) service was spun off from TF-CSIRT in 2001 and has become a widely known accreditation and listing service in the CERT community.[11]

TF-CSIRT was historically open to any interested CERT in Europe, but more recently has adopted the membership structure used by TI as part of formal incorporation of TI with TF-CSIRT. TF-CSIRT describes itself as 'a task force that promotes collaboration and coordination between CSIRTs in Europe and neighbouring regions, whilst liaising with relevant organisations at the global level in other regions'.[12]

TI describes itself as 'the trusted backbone of the Security and Incident Response team community in Europe', and serves as the 'listing, accreditation and certification service' of TF-CSIRT. Trusted Introducer provides two main services: (1) it keeps a list of all known European CERTs and (2) offers accreditation and certification services to CERTs. The idea behind TI's accreditation services – as well as its listing and certification services – is that these services help build up trust in the CERT community in Europe. Essentially, TI's stamp of approval allows other parties to assume with

[5] ENISA, Baseline Capabilities for National / Governmental CERTs (2009, 2010)
[6] ENISA, Deployment of Baseline Capabilities of National / Governmental CERTs: Status Report (2012); ENISA, Baseline Capabilities of National / Governmental CERTs: Updated Recommendations (2012)
[7] http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe
[8] http://www.enisa.europa.eu/activities/cert/support/exercise
[9] http://www.terena.org/activities/tf-csirt/
[10] http://www.terena.org/
[11] TERENA, Proposal for Restructuring TF-CSIRT and the Trust Introducer Service (December 2011)
[12] See TERENA website at www.terena.org

confidence that a CERT has reached a certain level of maturity and functionality, which is important to building trust throughout the CERT community.[13]

TF-CSIRT/TI offers three different mechanisms to European CERT: registration (listing), accreditation, and certification. Registration with TF-CSIRT/TI is a relatively simple process, while accreditation is more complex and certification even more so. Certification requires that a CERT meet a number of requirements laid out in the Security Incident Management Maturity Model published by TI.[14]

2.1.3 FIRST

The Forum of Incident Response and Security Teams (FIRST) was founded in 1990 as a worldwide network of individual computer security incident response teams that cooperate voluntarily to improve their abilities to deal with and prevent computer security problems. FIRST is a membership organisation that is governed by an Operational Framework, and each member must designate a primary and alternate representative to FIRST.

Participants in FIRST are part of a network of CERTs that work together voluntarily to deal with computer security problems and their prevention.

FIRST distinguishes between two types of participants:

- *Full members* represent organisations assisting defined constituencies in preventing and handling computer security-related incidents.
- *Liaison members* are individuals or representatives of organisations other than CERTs that have a legitimate interest in and value to FIRST.[15]

2.1.4 The Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is an open community of network designers, operators, vendors and researchers focused on the evolution of Internet architecture. IETF is divided into working groups based on topic area.[16] IETF published the RFC-2350 document, which is a detailed overview of the policies that it recommends a CERT pursues and the services that it is expected to offer. Although published in 1998 and last updated in 2003, RFC-2350 still enjoys widespread use as a reference document for CERT capabilities. RFC-2350 is an important document in the CERT community because a large number of CERTs use it as a template for the self-assessment.[17]The TI accredited and certified CERTs have adopted the RFC2350 as a basic requirement to fulfill.

2.1.5 CERT/CC

CERT Coordination Center (CERT/CC) is not a membership organisation in the same sense as FIRST or TF-CSIRT/TI, but it is still an influential organisation in the CERT community. CERT/CC was created in 1988 in response to the Morris worm incident,[18] and is hosted by Carnegie Mellon University within the Software Engineering Institute. This organisation actually established the first CERT in the world.

[13] See https://www.trusted-introducer.org/index.html
[14] See https://www.trusted-introducer.org/processes/overview.html
[15] See http://www.first.org/about
[16] See http://www.ietf.org/about/
[17] IETF, RFC-2350: Expectations for Computer Security Incident Response, available at http://www.ietf.org/rfc/rfc2350.txt
[18] http://en.wikipedia.org/wiki/Morris_worm

Under its charter, CERT/CC works with the Internet community in detecting and resolving computer security incidents by (1) providing a reliable, trusted, 24-hour, single point of contact for emergencies; (2) facilitating communication among experts; (3) serving as a central point for identifying and correcting computer system vulnerabilities; (4) maintaining close ties with research activities; and (5) being proactive in raising awareness about computer security issues. It is also involved in efforts to create standards in the CERT area, and has published open source tools for activities that include vulnerability assessment, network traffic analysis, and facilitating digital investigations.[19]

2.1.6 APCERT

The Asia Pacific Computer Emergency Response Team (APCERT) is an example of a CERT membership organisation that focuses on a particular region. According to APCERT, its purpose 'is to encourage and support coordination' among CERT organisations in the Asia-Pacific region. By doing this, it believes that it can 'improve the region's awareness and competency' with regard to computer incident response.[20]

APCERT is open to all CERTs in the Asia-Pacific region that meet its qualification criteria. APCERT members must also agree to support its objectives, respect information handling procedures, and, as much as possible, provide assistance to other APCERT members.[21]

2.1.7 International Organisation for Standardisation (ISO)

The International Organisation for Standardisation (ISO) is a non-governmental organisation that is made up of members from the national standards bodies of 163 countries. The ISO publishes standards developed by panels of experts on technical committees.[22] In 2011, ISO published a consensus-based standards document with its own guidelines for security incident management for large and medium-sized organisations. This publication, which is known as ISO 27035, purports to provide 'a structured and planned approach' to issues such as (1) detecting, reporting, and assessing information security incidents; (2) responding to and managing information security incidents; (3) detecting, assessing, and managing information security vulnerabilities; and (4) continuously improving information security and incident management as a result of managing information security incidents and vulnerabilities. ISO 27035 also provides guidance for external organisations providing information security incident management services.[23]

2.1.8 Other organisations

There are other organisations than the ones already discussed that have potentially suitable mechanisms. For example, many corporations have internal CERT capabilities that allow them to respond to incidents involving their products or services. These corporate-based mechanisms will often target the corporation's employees, business partners and internal lines of business.[24]

A different example is the European Government CERT Group (EGC Group),[25] an informal association of more mature governmental CERTs in Europe. EGC Group members cooperate effectively on matters of incident response while building upon mutual trust and understanding due to similarities

[19] http://www.cert.org/meet_cert/
[20] http://www.apcert.org/about/mission/index.html
[21] See Instructions for joining AP-CERT, available at http://www.apcert.org/application/index.html
[22] http://www.iso.org/iso/home/about.htm
[23] See http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379
[24] See for example http://tools.cisco.com/security/center/emergency.x?i=56
[25] http://www.egc-group.org/index.html

in constituencies and problem sets. EGC Group has a technical focus. EGC teams are usually members of FIRST and TF-CSIRT/TI.

2.2 Maturity assessment criteria

The CERT community organisations discussed above provide a number of different mechanisms for CERTs to use or to be part of. This section introduces the most important categories and topics that pertain to these mechanisms and provides the foundation for identifying commonalities and differences between them.

2.2.1 Type of approach (organisation model)

The approach adopted by a CERT community organisation is fundamental to its mechanism(s) and to how it interacts with CERTs. An organisation's approach is an important determinant of the relationships that it establishes with CERTs and the services that it provides. Organisations surveyed for this report employ several different approaches to how they interact with CERTs:

Type of organisation	Characteristics of the mechanism
Voluntary (good practice and recommendations)	The organisation is set up in a way that allows CERTs to participate in its processes and events, but it does not have a formal membership process. The organisation's focus is on providing good practices and recommendations, rather than providing confirmation of a CERT's capabilities or other services.
Subscribe (Membership and accreditation)	The organisation admits members through a formalised process. Its agenda and activities are driven by its status as a membership organisation. Membership in itself provides value through the receipt of member-only services, as well as through processes such as accreditation.
Compulsory (Standards)	The organisation has formal authority to require compliance with its mechanism(s) and often exists for the purpose of disseminating standards. Thus far, this approach has not been the norm for CERT community organisations, but the approach may be used more often as efforts are made to harmonise approaches and ensure that good practices are followed and the same level of capabilities is achieved.

The approach that these organisations employ provides information about matters such as:

- How an organisation interacts with CERTs, both members and non-members
- What member or associated CERTs can expect from an organisation
- What role an organisation envisions itself playing in the broader CERT community
- How an organisation sees itself growing and evolving over time
- Where an organisation can obtain operational and substantive input
- How an organisation secures funding.

2.2.2 Requirements for CERTs

A given organisation’s mechanism may impose requirements on CERTs seeking to utilise the mechanism or to associate with the organisation. Such requirements tend to reflect whether and to what extent the organisation in question wants to limit its involvement and whether it wants its

members to have similar capabilities and processes. Such organisations must also consider whether or not stringent requirements would deter otherwise strong partner or member CERTs from seeking involvement.

An organisation must also decide which specific requirements it will impose on CERTs in its mechanisms. Various approaches are open to an organisation in terms of implementing such requirements:

- Creating its own unique list of requirements that it expects a partner or member to meet
- Using an existing good practices guide for CERTs and requiring that a partner or member meet either all of these practices or a certain percentage of them
- Leaving the decision about cooperation with or involvement for a CERT to its existing members, and allowing them to decide by vote on whether the CERT meets its standards. It is up to the potential member (and possibly to its sponsors, which are already members of the respective organisation) to demonstrate to other members that the applicant CERT fulfils membership requirements.

2.2.3 Validation process

Organisations with membership requirements need a process by which to ensure these are met. For example, once a CERT becomes a member, it becomes more challenging for the organisation to backtrack and exert any control over the CERT.

An organisation can use different mechanisms to ensure that a CERT fulfils its requirements. There is usually some sort of initial phase where a CERT provides the organisation with baseline information about itself and its capabilities. This can then be checked against publicly available information about the CERT, or potentially by asking existing CERT members of the organisation to evaluate whether the applicant CERT meets the requirements.

The organisation has to decide whether it will put in place additional, more thorough means of validating a CERT's capabilities. This could include requiring more proactive input from the applicant CERT, including presenting its capabilities at a meeting of the organisation. Alternatively, on-site visits to the CERT are another way to measure capabilities and resources, although this involves more expense. There is also a distinction between processes where validation takes place at one point in time (e.g. FIRST) or whether it is a continuing process (e.g. TI accredited/certified).

2.2.4 CERTs' focus: type and region

The organisation also determines which types of parties it wants as members or users of its services. There are advantages in having members with similar patterns or goals, both of which can be influenced by factors such as geography or type of the constituency.

When it comes to the type of the CERT, there are a number of identified sectors that an organisation could focus on. For a non-comprehensive list see the table below.

CERT Types: Sector[26]
National / Governmental
Governmental
National
De facto national
Research and education
Governmental / Military
Service provider/ISP customer base
Non-commercial organisation
ICT vendor customer base
Commercial organisation
Financial sector
Energy sector
Industrial sector
Other...

This can either be done at an abstract level – e.g., academic or commercial CERTs – or through a more concrete association with a corporation. This type of organisational limitation means that CERTs seeking membership or association will tend to share common business models, concerns about cyber-security, use of same technologies, and can be expected to have and use good practices that apply across the specific constituency base. In terms of geography, CERT organisations can either be open or be limited to specific geographic areas.

Limitations based on geography most often are set at a regional or country level, but could also be set for a specific region or even a city within a country. Covering a specific geographic area enables a CERT organisation to have member CERTs and constituents who share similar constituencies, have the same legal code or agreed legal framework (e.g., EU Directives) or face common cultural and linguistic challenges, and similar patterns of interactions with their governments. It may also facilitate very important face-to-face meetings.

[26] Updated ENISA list of CERTs available at: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

2.2.5 Benefits and added value of a mechanism

A mechanism has to offer value to its CERT members or the CERTs that utilise it. This value can take a number of forms:

Benefit/Value	What it means
Affirmation	Value comes from organisation's/ mechanism's ability to provide trusted, independent, third-party confirmation of a CERT's capabilities.
Contractual Requirements	Value comes from organisation's/ mechanism's ability to provide certification of a CERT's capabilities that it needs for contractual or regulatory reasons.
Recognition	Value comes from the desire by the CERT to be recognised for the status it has achieved and the fact that the mechanism can provide this recognition widely.
Good practices	Value comes from good practices that these organisations/ mechanisms can provide based on their strong platforms, visibility and recognition.
Services	Value comes from specific services that the organisation provides.
Networking	Value comes from the opportunity these organisations can offer their members to network with other CERTs and players.
Growth opportunities (Maturity)	Value comes from these organisations offering CERTs the chance to grow their teams through training and other exercises, or by helping them establish clear goals for developing their teams.

2.2.6 Definitions and terminology

The definitions and terminology that are used are important within the mechanisms. Precise definitions are often needed to make clear issues that are at the heart of CERTs' missions. These definitions lay the foundation for the capabilities that CERTs will provide and how they will otherwise conduct their business.

It is also important that organisations provide an overview of the types of specific definitions and terminology that CERTs are expected to follow. These need not always be defined as tightly as some other foundational terms, but they will often be at the heart of what a CERT does, and thus it is important that expectations be stated clearly for it in this regard (e.g. n/g CERT definitions and terminology put forward by ENISA or TF-CSIRT/TI).

2.2.7 Keeping the mechanism up to date

An organisation's mechanism needs to be updated once it is put in place, which in turn requires that a number of decisions are taken. One such decision is whether updates will be considered on a regular basis at a defined time, or on an ad-hoc basis. This will influence how an organisation considers changes and the likelihood of such changes being adopted.

Another question is how mechanisms will be updated. This relates to topics such as how potential changes will be brought up for consideration, which bodies or individuals will consider and make decisions about changes, what the standards for adopting updates or changes are, and how

information about updates or changes will be disseminated to members or other CERTs associated with the organisation.

An organisation also has to decide how much input CERT teams will have in developing and updating their capability mechanism. The advantage of giving CERTs input is that the capability mechanism is then more likely to reflect the issues CERTs see as important, and will also increase the odds that they will accept and follow the mechanism. On the other hand, opening up an organisation's mechanism broadly to input from CERTs risks moving the organisation away from its core focus and could lead to disagreement between members.

2.2.8 Promoting the mechanism and CERTs' training

CERT community organisations promote and advertise their capability mechanisms to different extents. For some of them, promoting their mechanism is fundamental to their existence (e.g. FIRST): their capability has to resonate within the CERT community, or there is really no reason for a CERT to try to become a member of an organisation or associate with it. On the other hand, creators of other mechanisms discussed in this report are less concerned with promoting their mechanism, and may be satisfied with just creating a mechanism and then letting CERTs decide whether they want to use it or adopt it (e.g. ISO model, RFC2350). CERTs and other stakeholders can also be important disseminators of information about a particular capabilities mechanism, although their willingness to engage in promotion will probably depend on their connections to the mechanism and the extent to which they use the mechanism.

Organisations can follow two primary approaches in promoting themselves and their mechanisms. First, they can do it themselves. This requires that they devote the necessary resources and establish the right connections in the media to distribute information about their capabilities. Second, organisations can rely on their CERT members, stakeholders, and other bodies in the area of cyber-security to promote their mechanism. This can be more effective than self-promotion and costs less, but it is also riskier. This requires that an organisation have the right lines of communication open with key stakeholders and other parties and make the effort to track its publicity from these types of third parties.

Training programmes and exercises are also a core element of what some organisations do, and training is an area where clear demand exists from CERTs and other players in the CERT arena. Both CERTs and their constituents will rely on training offered by organisations as well as conferences and other educational programmes that CERT organisations offer.

Organisations thus have to make decisions about the types of training they will offer, who they will offer this training to, and the extent to which their membership bases or constituencies will drive the content of the training that they offer. Given often limited resources, this may present a challenge to some organisations and CERT teams, but the importance of these member and constituent services mean that they cannot be overlooked.

3 CERT Maturity Model

A CERT's development occurs broadly as a three-stage progression in which it moves from being established to achieving a complete set of capabilities and stability within its community. At each stage of this progression, mechanisms from CERT community organisations can provide guidance and support to CERTs with regard to the assessment categories discussed in section 2.2 of this document.

For the purpose of this document we applied a three-tier maturity model, which is based on the ongoing work of the FIRST Education Committee.[27] Individual mechanisms of CERT organisations are attached to the three tiers with basic pre-defined characteristics. The mechanisms of the three Tiers are then further explored in section 4 using a set of eight criteria.

CERT MATURITY MODEL			
	Summary	**Characteristics**	**Organisation / Mechanisms**
Tier 1	*Fundamental* (Essential, indispensable)	CERT is being established and trying to earn recognition in the CERT community (based on individual trust building).	ENISA: *A Step-by-Step Approach on How to Set up a CSIRT* (2006) ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009) ENISA: *Map of CERTs* and *Inventory of CERT Activities in Europe* (2005, constantly updated) RARE CERT Task Force[28]: *Guide to Setting up a CERT* (1993) TF-CSIRT/TI: *'Listed' status*
Tier 2	*Baseline* (Steady, Sure-Footed)	CERT has baseline capabilities (operations) in place and its team representative gained trust among the CERT community.	ENISA: *Baseline Capabilities for National/ Governmental CERTs – Policy recommendations* (2010, 2012) IETF: RFC-2350 (2003 updated) TF-CSIRT/TI: 'Accreditation' FIRST: 'Full Membership' APCERT: 'Membership' CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)
Tier 3	*Advanced* (Stable, Well-Balanced)	CERT has a complete set of capabilities in place and has established a	ENISA: *n/g CERT standard capabilities mechanism* (2014) ISO: *ISO 27035* (2011 update)

[27] http://www.first.org/about/organization/committees#edc
[28] http://www.terena.org/activities/tf-csirt/archive/acert7.html

		stable place in the community (no longer dependent on individuals from the team). These capabilities are all documented.	TF-CSIRT/TI: ‘Certification’

4 CERT mechanisms under the spotlight

This section provides a more detailed overview of the mechanisms that organisations offer to CERTs in each of the three tiers (as described above in the CERT Maturity Model). This overview in the form of tables should not be considered as a ranking of mechanisms as they are very different in nature. For example, some of them are membership-based, while others take the form of guidelines and/or recommendations for interested CERTs to follow. ENISA has identified the following eight categories for the analysis of the individual mechanisms.

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

4.1 Tier 1 of the CERT Maturity Model

CERTs that are currently in Tier 1 are in the process of being established and gaining initial recognition in the CERT community. CERT community organisations' mechanisms can thus provide Tier 1 CERTs with valuable guidance in terms of getting set up, establishing fundamental operations, and helping to earn initial recognition within the CERT community.

The following mechanisms identified for Tier 1 were considered also for the analysis of commonalities and differences of CERT mechanisms:

- ENISA: *A Step-by-Step Approach on How to Set up a CSIRT* (2006)
- ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)
- ENISA: *Inventory of CERT Activities in Europe – CERT Inventory Map* (2005)
- RARE CERT Task Force: *Guide to Setting up a CERT* (1993)
- TF-CSIRT/TI: 'Listed' status

4.1.1 Type of approach (organisation)

The five mechanisms identified for Tier 1 rely on fundamentally different organisational approaches. Most importantly, ENISA do not use membership approaches at this level, while TF-CSIRT/TI is a membership-based organisation. In addition, ENISA seeks to provide capabilities mechanisms to CERTs even without a formal membership structure. That said, ENISA was established by the European Union (EU) to improve network and information security in the EU, and takes a proactive stance in serving as a facilitator and information broker for CERTs in EU Member States. Meanwhile, TF-CSIRT/TI's mechanism is membership-based even at the Tier 1 level, although the criteria that a

CERT must meet to obtain the 'Listed' status with TF-CSIRT/TI are less exacting at the earliest stage than they become as the CERT's maturity level increases.[29] All of these mechanisms are provided on a non-profit and voluntary basis.

Tier 1 Mechanism	Type of approach (organisation)	Voluntary/ subscribe / compulsory form
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	This is universal step-by step-guidance on how to set up a CSIRT. The target groups are governmental as well as other institutions that decide to set up a CERT to protect their own infrastructure or that of their stakeholders.	Voluntary (good practices and recommendations)
ENISA: *Baseline Capabilities for National/ Governmental CERTs – operational aspects* (2009)	This mechanism was defined in 2009 for newly established n/g CERTs to help them understand and focus on a basic set of capabilities so as to facilitate efficient and effective incident response and collaboration.	Voluntary (good practices and recommendations)
ENISA: *Inventory of CERT Activities in Europe (2005, constantly updated)*	This mechanism was developed by ENISA in 2005 and gives the newly established team an opportunity to gain recognition among teams in Europe and other stakeholders ENISA with which closely cooperates.	Voluntary (good practices and recommendations)
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	This mechanism was created in 1993 by the CERT Task Force to 'offer guidance to networking organisations who wish to set up CERTs' and thus takes a voluntary approach.	Voluntary (good practices and recommendations)
TF-CSIRT/TI: 'Listed' Status	TF-CSIRT/TI is a formal membership organisation open to all recognised CERTs situated in Europe, while CERTs seeking to achieve 'listed' status with TF-CSIRT/TI must meet baseline requirements.	Voluntary (after meeting pre-defined requirements/criteria offers the 'listed' status)

4.1.2 Requirements for CERTs

Because ENISA is not a membership organisation, it generally does not place requirements on CERTs seeking to utilise its mechanisms, although ENISA's *Inventory of CERT Activities in Europe* is based closely on TI database updates. On the other hand, TF-CSIRT/TI offers three levels of membership classes, with the first level – Listing – being most applicable to Tier 1 CERTs. TF-CSIRT/TI allows any organisation that has implemented a security or incident response capability or which provides incident management services to register with it for listing. TF-CSIRT/TI does not further define this

[29] Information from ENISA, CERT/CC, and TI homepages or reports

requirement, which suggests a relatively low bar for CERTs wanting to achieve listed status under its mechanism.[30]

Tier 1 Mechanism	Requirements for CERTs
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	This mechanism does not place requirements on CERTs intending to use it. Even though ENISA's focus is on CERTs in Europe, this guidance has proved its usability far behind the European borders.
ENISA: *Baseline Capabilities for National / Governmental CERTs* – operational aspects (2009)	This mechanism does not place requirements on CERTs intending to use it.
ENISA: *Inventory of CERT Activities in Europe* (2005, constantly updated)	This mechanism lists CERT teams in Europe, and tries to 'give a profile of the situation concerning CERT teams and their activities in Europe.' ENISA's inventory listing is largely based on TI membership.
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	This mechanism does not place requirements on CERTs intending to use it.
TF-CSIRT/TI: 'Listed' Status	This mechanism requires that an applicant for seeking 'listed' status have implemented a security or incident response capability or provide incident management services.

4.1.3 Validation process

ENISA does not have formal mechanisms for evaluating CERTs' capabilities. In 2012 ENISA carried out follow-up assessments of whether n/g CERTs in Member States are following its baseline recommendations, based on a survey of these organisations and desk research. TF-CSIRT/TI has a validation process in place for its initial stage of membership: it requires that an applicant for listing have the support of at least two existing members and notes that 'if there is no support (for the candidate) – or if there are even objections – the candidate will not be accepted'.[31]

Tier 1 Mechanism	Validation process
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	There is no validation process associated with use of this mechanism.
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	There is no validation process associated with use of this mechanism.
ENISA: *Inventory of CERT Activities in Europe* (2005,	This inventory of CERTs is updated based on discussions with CERT teams and the latest CERT team updates on Trusted Introducer's

[30] https://www.trusted-introducer.org/processes/registration.html
[31] https://www.trusted-introducer.org/processes/registration.html

constantly updated)	website, although other sources such as FIRST and TF-CSIRT are also considered.
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	There is no validation process associated with the use of this mechanism.
TF-CSIRT/TI: 'Listed' Status	This mechanism requires an applicant for listing to have the support of at least two existing members (accredited teams only) and notes that if the candidate has no support or if any objections to the candidate are raised, the candidate will not be accepted.

4.1.4 CERTs' focus: type and region

ENISA's mandate makes clear that its focus is on CERTs in EU Member States, especially n/g CERTs, and its revised mandate has provided it with an even broader purview in the area of cyber-security in Europe. While ENISA works intensively with CERTs in EU Member States as they are set up or as they extend their capabilities, it also publishes significant amounts of information about these topics that could be useful for CERTs in similar positions anywhere. TF-CSIRT/TI describes itself as 'the trusted backbone of the security and incident response team community in Europe', making clear that its activities are also focused on Europe. This includes organisations and teams that work on a global level or have a stake in Europe.

Tier 1 Mechanism	CERTs' focus: type and region
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	all types of CERTs/Europe
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	n/g CERTs in EU Member States
ENISA: *Inventory of CERT Activities in Europe* (2005, constantly updated)	all types of CERTs/Europe
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	all types of CERTs
TF-CSIRT/TI: 'Listed' Status	all types of CERTs/Europe

4.1.5 Benefits and added value of the mechanism

Organisations with useful mechanisms for Tier 1 CERTs offer varied benefits and value to CERTs. ENISA's work in helping CERTs get off the ground is in line with its broader goal of 'assisting EU Member States in implementing relevant EU legislation and working to improve the resilience of Europe's critical infrastructure and networks'.[32] Thus, the value that CERTs take from ENISA is

[32] ENISA, Deployment of Baseline Capabilities of National / Governmental CERTs: Status Report (2012) at p. 3.

through good practices and other advice on how to establish themselves and improve their capabilities. It also enables EU Member States to gain assurance of compliance with relevant communications of the EU Commission and recommendations of other EU institutions.

At this stage of a CERT's development, RARE CERT Task Force provides value to CERTs largely through its good practices related to establishing a CERT, including topics such as defining a constituency and developing a mission statement. TF-CSIRT/TI's value is slightly more diverse: it offers baseline recognition of a CERT's capabilities, along with the promise of potentially greater recognition as the CERT develops.

Tier 1 Mechanism	Added value of the mechanism
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	This mechanism provides value through good practices to its target audience. It is very useful when building a CERT from scratch as it lists all the steps necessary in the process of setting up a CERT.
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	This mechanism provides value through good practices to its target audience. It enables the n/g CERTs in the EU to take part in modification of this mechanism based on their experience and needs. ENISA offers various platforms for the engagement of n/g CERTs including CERT workshop and stocktaking reports. Additional added value of the mechanism is that Member States establishing n/g CERTs gain assurance of compliance with respective communications and recommendations of the EU Commission and other EU institutions.
ENISA: *Inventory of CERT Activities in Europe* (2005, constantly updated)	This mechanism offers value to CERTs listed by validating their position as publicly listed CERTs, and through the information it offers about CERTs in Europe and international CERT initiatives (a very comprehensive and publicly available list of all kinds of CERTs).
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	This mechanism provides value through good practice to its target audience.
TF-CSIRT/TI: 'Listed' Status	This mechanism offers baseline recognition of a CERT's capabilities, along with the promise of greater potential recognition as the CERT develops, as well as a CERT starter kit through TF-CSIRT. The information on the teams is accessible via web, while detailed information including contacts and access to operational services are reserved for the members.

4.1.6 Definitions and terminology

The organisations that actively support Tier 1 CERTs offer definitions of key CERT terms which differ slightly. Their definitions are similar in key ways, such as that they all mention operational capabilities like incident response service and assume that a CERT will provide these services to a defined constituency. ENISA specifies that a CERT's 'main business is to respond to computer security incidents'.[33] Meanwhile, RARE CERT Task Force defines a CSIRT/CERT as an organisation that receives, reviews and responds to computer security incident reports and activity.

[33] ENISA, A Step-by-Step Approach on How to Set up a CSIRT, at p. 7.

These organisations also have similar core conceptualisations of what a CERT's constituency is: in essence, that a CERT must have a defined 'customer base' that it serves. Beyond this similarity, though, there are differences. ENISA takes a broad purview on this potential customer base, which is in line with its focus on n/g CERTs, but focuses on choosing the right communication channels for reaching constituents.[34] TI's form for new registration candidates does not define constituency but requires applicants to describe their constituency 'based on a description of Internet Domains, IP Address Information and/or other suitable characterization of the constituency'.[35] Similarly, all organisations give examples of CERT types, while ENISA's *Inventory of CERT Activities in Europe* is the most comprehensive in this respect.

Tier 1 Mechanism	Definitions and terminology		
	CERT/CSIRT definition	**Constituency definition**	**CERT type categories and definitions**
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	*CSIRT*: 'a team of IT security experts whose main business is to respond to computer security incidents'	*Constituency*: 'the customer base of a CSIRT', definitions for the constituencies of various CERT categories also included (see the next column in this table)	These sectors are listed (in alphabetical order) with definitions included (pages 8–10): • Academic • Commercial • CIP/CIIP Sector • Governmental Sector • Internal • Military Sector • National • Small & Medium Enterprises (SME) • Vendor
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	*CERT*: 'a team of IT security experts whose main business is to respond to computer security incidents'[36]	*Constituency:* 'an established term for the customer base (of a CERT)'	The mechanism defines main CERT categories of its focus: • national • de facto national • governmental • national/governmental Besides, other CERT categories are mentioned (academia, companies, or military) with regard to various constituencies without any further definition.
ENISA: *Inventory of CERT Activities in Europe*	*CERT*: 'an organisation that studies computer and network	A number of various CERT constituencies are listed without any further definition. (see	*N/g CERT teams*: 'all "flavours" of national CERTs, governmental CERTs, national points of contact and others in the EU Member States.'

[34] ENISA, A Step-by-Step Approach on How to Set up a CSIRT, at p. 7.
[35] See Application form for Listed candidates, available at https://www.trusted-introducer.org/list_v23.txt
[36] The term CSIRT is a more modern synonym and should reflect the fact that CERTs developed over time from being mere reaction forces to become more universal providers of security services.

(2005, constantly updated)	security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.'	section 2.2.4)	A number of various CERT categories are listed without any further definition. (see section 2.2.4)
RARE CERT Task Force: ***Guide to Setting up a CERT (1993)***	*CSIRT*: 'a central capability for analysing events, co-ordinating technical solutions, ensuring that necessary information is conveyed to those who need such information, and training others to deal with computer security incidents'	*Constituency:* 'refers to the concept of a CERT whose constituency is a network of affiliated computing sites with a valid computer security policy'	Not specific about CERT categories but a lot of attention is paid to vendor CERTs (which is understandable due to the age of this mechanism)
TF-CSIRT/TI: 'Listed' Status	Own definition is not used but it liaises with other organisations like FIRST (specifically mentioned in the registration procedure) and ENISA.	The same applies here as regards constituency, which is 'based on a description of Internet Domains, IP Address Information and/or other suitable characteristics'	The mechanism lists the following CERT categories (relevant also for constituencies): • ISP Customer Base • Service Customer Base • Vendor Customer Base • Commercial Organisation • Financial Sector • Government • Military • Non-Commercial Organisation • Research & Education

			Network There are brief specifications of some of these CERT categories.

4.1.7 Keeping the mechanism up to date

None of these organisations specify how they keep their mechanisms updated. ENISA has stated that its work in this area 'should be considered only as a first step towards the specification of requirements, which is an ongoing process that has and will involve discussions with the relevant stakeholders in the Member States'.[37] TI's mechanism is about recognising a CERT's status and the development of TI mechanism is described in details under service governance section of the TI contact description[38].

Tier 1 Mechanism	Keeping the mechanism up to date
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	This mechanism does not make specific provisions for keeping it up to date, although ENISA generally considers its good practices to be works in progress.
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	This mechanism does not make specific provisions for keeping it up to date, although ENISA generally considers its good practices to be works in progress.
ENISA: *Inventory of CERT Activities in Europe* (2005, constantly updated)	This mechanism notes that 'to be really useful in the future, this document has to be updated: obsolete information will have to be deleted; information about new teams and activities will have to be validated and added' (pp. 42–43). It therefore requests that changes, mistakes, or additions be provided to ENISA. The CERT inventory is updated twice a year on a regular basis in Q2 and Q4. There is also a possibility for an ad-hoc update based on a team's request.
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	This mechanism does not make specific provisions for keeping it up to date.
TF-CSIRT/TI: 'Listed' Status	In the section 9 of the ToR 2012, it is stated that requirements for this status are defined by the Review Board and also could be changed by the TI Community.[39]

4.1.8 Promoting the mechanism and CERTs' training

These organisations take different views on topics such as promoting their mechanisms and training CERTs in Tier 1 of the Maturity Model. ENISA holds an annual '*CERTs in Europe*' workshop where

[37] http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-for-national-governmental-certs(p. 5)
[38] https://www.trusted-introducer.org/contact.html
[39] http://www.terena.org/activities/tf-csirt/publications/ToR-2012.pdf

experiences, good practices and 'TLP red[40] discussion' are shared, and where ENISA updates CERTs about its efforts.[41] ENISA is also active on the training front, and considers training and exercising CERTs to be one of its core missions.[42] It offers training programmes and workshops for CERTs at different developmental stages, including those being established or introduced to their constituents. ENISA continuously supports the TRANSITS training programme.[43]

TF-CSIRT/TI is also proactive when it comes to promoting their mechanisms. The TI service provider is tasked, by service specification and Steering Committee, to actively look out for potential listing candidates. They monitor the FIRST memberships and follow up with suggestions from fellow teams. When it comes to training, TF-CSIRT/TI is involved in the provision of TRANSIT I training courses popular within the CERT community. On 30 July 2013 TF-CSIRT/TI (via TERENA) and FIRST signed a Memorandum of Understanding (MoU) regarding the use and promotion of TRANSITS I security training materials worldwide.[44]

Tier 1 Mechanism	Promoting the mechanism and CERTs' training
ENISA: *A Step-by-Step Approach on How to Set Up a CSIRT* (2006)	This mechanism does not make provisions for its promotion. In terms of training, it lists TRANSITS and CERT/CC courses as the two main sources for dedicated training that CERTs should use.
ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009)	This mechanism does not make provisions for its promotion or with regard to training. But it does refer to training in general terms under the guidelines.
ENISA: *Inventory of CERT Activities in Europe* (2005, constantly updated)	Promotion is carried out by means of ENISA's main activities as a broker between different Network and Information Security communities (events, presentations, etc.)
RARE CERT Task Force: *Guide to Setting up a CERT* (1993)	This mechanism does not make provisions for its promotion.
TF-CSIRT/TI: 'Listed' Status	This mechanism offers training courses for new and experienced personnel through TRANSITS I, which are organised by TERENA and regularly supported by ENISA. There are no specific provisions for promoting the mechanism, although there are regular open meetings (held three times a year) with the right to access for Listed teams.

[40] http://en.wikipedia.org/wiki/Traffic_Light_Protocol
[41] http://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-I
[42] Extensive online training and exercise material is available at http://www.enisa.europa.eu/activities/cert/support/exercise.
[43] See for example the 2013 ENISA Work Programme: http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013.
[44] http://www.terena.org/news/fullstory.php?news_id=3465

4.2 Tier 2 of the CERT Maturity Model

CERTs that fall in Tier 2 of the CERT Maturity Model have established themselves in terms of having baseline operational capabilities and a cooperative relationship within the CERT community. The team representative enjoys trust in the wider CERT community. Thus, these CERTs will look to community CERT organisations for affirmation of their existing capabilities as well as good practices for further developing their capabilities and deepening their relationships with their constituents and communities.

The following mechanisms are recognised for Tier 2 CERTs and were considered for the analysis of commonalities and differences of CERT mechanisms:

- ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012)
- Internet Engineering Task Force: RFC-2350 (2003 updated)
- TF-CSIRT/TI: 'Accredited' status
- FIRST: 'Full Membership' status
- APCERT: 'Membership' status
- CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)

4.2.1 Type of approach (organisation)

The six organisations with mechanisms geared towards Tier 2 CERTs have a variety of commonalities and differences in their approaches. Membership organisations are more prevalent at this level; TF-CSIRT/TI, FIRST and APCERT are all member-based organisations. As discussed previously, ENISA is not membership based, but exists for the benefit of all CERTs in EU Member States. Meanwhile, the IETF is an open organisation that focuses on good practices.

FIRST and TF-CSIRT/TI are membership-based organisations with relatively formalised processes in terms of management structure and other internal processes. TF-CSIRT/TI, for example, holds membership meetings three times per year, with its Review Board 'overseeing and steering' TI's activities. Meanwhile, FIRST has an operational framework that lays out the organisational structure and basic organisational policies, as well as bylaws that explain formalities such as meetings and the election of directors. FIRST holds an annual general meeting in accordance with its operational framework.[45] APCERT is also a membership organisation that holds an annual meeting open to all of its members of any class. At this meeting, APCERT's Steering Committee is elected, which is responsible for APCERT's general operating policies, procedures, guidelines, and other matters affecting APCERT as a whole.[46]

There is a noticeable difference in the approach of CERT community organisations that focus on CERTs further along in the maturation process than for those just getting started. This tendency towards member-based structures makes sense, as CERTs which will become members of these organisations have reached a level of maturity that allows them to provide insight to other CERTs and help the organisation better serve its members.

[45] FIRST Operational Framework, available at http://www.first.org/about/policies/op-framework

[46] AP-CERT Operational Framework, available at http://www.apcert.org/documents/pdf/OPFW_26March2013.pdf

Tier 2 Mechanism	Type of approach (organisation)	Voluntary/ subscribe/ compulsory form
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	This mechanism was defined in 2010 for newly established n/g CERTs to help them understand and focus on a basic set of capabilities so as to facilitate efficient and effective incident response and collaboration. It was then updated in 2012 with a review of the baseline set of capabilities of n/g CERTs in EU MS.	Voluntary (targeted EU policy recommendations)[47]
IETF: RFC-2350 (2003 updated)	This mechanism was initially created in 1998 and updated in 2003 as an effort to 'express the general Internet community's expectations' of CERTs. As such, it serves as a voluntary mechanism based on good practices for CERTs.	Voluntary
TF-CSIRT/TI: 'Accreditation'	This mechanism is formal and membership-based, with formalised processes for accepting members and internal processes.	Subscribe
FIRST: 'Full Membership'	This mechanism is formal and membership-based, with formalised processes for accepting members and internal processes.	Subscribe
APCERT: 'Membership'	This mechanism is formal and membership-based, with formalised processes for accepting members and internal processes.	Subscribe
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	This mechanism was created in 1993 to 'offer guidance to networking organisations who wish to set up CERTs' and thus takes a voluntary approach.	Voluntary/good practice

4.2.2 Requirements for CERTs

As noted, ENISA is not a membership organisation, so it does not issue requirements for CERTs seeking to associate with it, even though it publishes good practices and recommendations for CERTs. The IETF is an open organisation without requirements for entities wanting to associate with it.

[47] As stipulated in the Communication of the European Commission entitled 'A Digital Agenda for Europe' COM(2010) 245 final, EU Member States should have established a well-functioning network of CERTs at national level covering all of Europe by 2012: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML

Unlike the approaches of ENISA, IETF and CERT/CC, the other three organisations analysed in this section all have requirements for gaining membership.

FIRST does not require that a CERT have specific capabilities to become a member, but it suggests that a CERT should meet a solid majority of a list of recommended criteria. Uniquely, FIRST requires that applicants agree to host a site visit from an appointed FIRST team to 'ensure that the candidate CSIRT meets all needed requirements to be an active and beneficial member of FIRST'.[48]

TF-CSIRT/TI allows listed members to then apply for accreditation with it. To gain accredited status, a CERT is obliged to meet certain requirements, with the RFC-2350 document serving as the basis for the capabilities that an accredited CERT should have. The applicant CERT must formally apply (which entails set procedures) and provide information such as a list of the services it provides, its staffing resources, and policies regarding information handling.[49]

APCERT requires that operational member candidates meet a number of membership criteria, ranging from performing CERT functions on a full-time basis to being at least partly government-funded. Candidates must also maintain the confidentiality of information shared with other members, actively share information with other members, respond to inquiries in a timely manner, and participate in APCERT activities and initiatives.[50]

Tier 2 Mechanism	Requirements for CERTs
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	This mechanism does not directly impose requirements on CERTs wishing to adopt its mechanism or otherwise use its good practices contained in these documents. On the other hand, the recommendations contained in the document are crucial for attaining the goal of having a well-established network of n/g CERTs in Europe by 2012. See footnote 47.
IETF: RFC-2350 (2003 updated)	The mechanism outlined in this publication is from an open organisation – an organisation without requirements for entities that want to associate with it or to follow the good practices contained in RFC-2350.
TF-CSIRT/TI: 'Accreditation'	This mechanism requires CERTs seeking accredited status to meet certain requirements, with the RFC-2350 document serving as the basis for reviewing their capabilities. The applying CERT must fill out an application package and provide information such as a list of the services it provides, its staffing resources, and policies regarding information handling
FIRST: 'Full Membership'	This mechanism does not include specific required capabilities for membership, but provides a list for analysing a CERT's capability and notes that a CERT should have most of these capabilities. The mechanism also includes a site visit from an appointed team to confirm the CERT's capabilities.

[48] FIRST Site Visit Requirements and Assessment, available at http://www.first.org/membership/site-visit-V1.0.pdf
[49] http://www.trusted-introducer.org/processes/accreditation.html
[50] AP-CERT Operational Framework, available at http://www.apcert.org/documents/pdf/OPFW_26March2013.pdf, at p. 3

APCERT: 'Membership'	This mechanism requires that CERTs seeking Operational Member status meet a number of membership criteria. Applicants must also maintain the confidentiality of information, actively share information with other members, respond to inquiries in a timely manner, and participate in activities and initiatives of the mechanism.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	This mechanism does not place requirements on CERTs intending to use it.

4.2.3 Validation process

ENISA does not have a formal mechanism for evaluating CERTs, although it monitored in 2012 whether n/g CERTs in EU Member States are following its baseline recommendations.[51] Likewise, the IETF and CERT/CC do not concern themselves with validating the capabilities of CERTs following their mechanism.

FIRST and TF-CSIRT/TI mechanisms both have well-established processes for validating the capabilities of CERTs applying for their mainstream membership classes. TF-CSIRT/TI requires that an applicant must prove its capabilities based on the RFC-2350 document to gain membership, and notes that 'a team has to provide a useful, but limited, amount of operational information'. The TF-CSIRT/TI accreditation process then focuses on the authenticity, actuality, and correctness of the information provided, which is done either by personal discussion with a member of a team or through a cryptographic connection.[52] FIRST requires applicants for full membership to be nominated by two existing full members of FIRST and to then be approved by a two-thirds vote of its Steering Committee, as well as be subjected to the site visit discussed above.[53] APCERT's validation process is less clear and it does not explicitly lay out how it enforces the requirements mentioned in the previous section.

This means that CERTs accepted for membership by these organisations have a certain status within the broader CERT community and have reached baseline level of capabilities before they are allowed to become members and associate themselves with these CERT community organisations.

Tier 2 Mechanism	Validation process
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	The objective of the updated version of the reports was to measure the extent to which n/g CERTs in EU Member States have met the baseline capabilities identified. See the 'Deployment of baseline capabilities of national/governmental CERTs – Status Report 2012'.[54]
IETF: RFC-2350 (2003 updated)	The mechanism outlined in this document does not involve validating the CERT capabilities.

[51] ENISA, Deployment of Baseline Capabilities of National / Governmental CERTs: Status Report (2012)
[52] http://www.trusted-introducer.org/Template-Invitation-for-Accreditation_v20.pdf
[53] http://www.first.org/about/policies/op-framework, under FIRST Participation
[54] http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012

TF-CSIRT/TI: 'Accreditation'	This mechanism's validation process is based on an applicant proving its capabilities based on the RFC-2350 document to gain membership. The mechanism requires that a team demonstrate the authenticity, actuality and correctness of information it provides in support of its application (every four months an accredited team needs to confirm its data or will be asked to do so).
FIRST: 'Full Membership'	This mechanism requires applicants for full membership to be nominated by two existing full members and to then be approved by a two-thirds vote of the Steering Committee, as well as meeting the requirements of the site visit discussed above.
APCERT: 'Membership'	The documentation from this process does not explicitly state how the organisation enforces its membership requirements.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	No validation process is associated with use of the mechanism outlined in this document.

4.2.4 CERTs' focus: type and region

By geographic focus, ENISA and TF-CSIRT/TI focus on CERTs in Europe, as previously discussed, while APCERT was established to benefit CERTs from Asian-Pacific countries. FIRST is an international organisation that seeks and accepts members from around the world. There is little to suggest that the geographic scopes of these organisations have a significant impact on their status in the CERT community or the services that they provide.

Likewise, none of these organisations have limited their activities to particular industries, even if they sometimes carry out vertical-specific analyses or training sessions.

Tier 2 Mechanism	CERTs' focus: type and region
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	n/g CERTs from EU Member States
IETF: RFC-2350 (2003 updated)	all types of CERTs/global
TF-CSIRT/TI: 'Accreditation'	all types of CERTs in Europe or with valid interests in EU
FIRST: 'Full Membership'	all types of CERTs/global
APCERT: 'Membership'	all types of CERTs/Asia-Pacific region
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	all types of CERTs/global .

4.2.5 Benefits and added value of the mechanism

The benefits that CERTs gain from implementing the mechanisms in the Tier 2 level of the CERT maturity model change as their maturity levels increase. In particular, gaining 'Accredited' status with TF-CSIRT/TI or full membership with FIRST suggest that a CERT has reached a stage in its development where it has capabilities typically associated with CERTs. This is a key value of these organisations: when a CERT is granted a certain status with one of these organisations, then the CERT in question has clearly met certain requirements; outside parties can count on TF-CSIRT/TI or FIRST's expertise in such matters. CERTs that reach the accredited status with TF-CSIRT/TI will have already been listed members, while those gaining full membership with FIRST will have been subjected to a site visit, suggesting that these CERTs will be well-known entities to these organisations by the time they gain such a membership status.

All of these CERT organisations can also recommend good practices to CERTs or other interested parties as they improve their capabilities. Like ENISA, these organisations have issued mechanisms that roughly mirror ENISA's baseline capabilities mechanism. These organisations divide their mechanisms slightly differently:

- ENISA: Mandate capabilities; Operational capabilities (technical); Operational capabilities (organisational); Co-operational capabilities
- TI: Organisation; Human Resources; Processes; and Tools
- FIRST: Operational Requirements; Policies; Workplace/Environment; Incident Handling
- RFC-2350: CERT Scope; Policies and Procedures; Cooperation; Services

There are also other elements to these mechanisms' value. For example, TF-CSIRT/TI lists several other value-added services that accredited teams can benefit from:

- Access to members-only parts of the TF-CSIRT/TI website;
- Access to certain mailing lists only available to accredited teams;
- Access to value-added information only available to accredited teams;
- Access to in-band and out-of-band alerting services; and
- Access to TF-CSIRT/TI meetings restricted to accredited teams only.[55]
- Voting privileges: if a vote is needed (elections, rule changes, community topics), only accredited teams can take part in the vote.
- Nomination privileges: only accredited teams can nominate candidates for the Steering Committee.

FIRST also similarly provides what it terms 'value added services', including dedicated mailing lists with access to good practice documents, technical colloquia, classes, an annual incident response conference, as well as various presentations.

[55] Invitation Package for TI 'Accredited Status', at p. 5.

Tier 2 Mechanism	Benefits and added value of the mechanism
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	Baseline capabilities for all n/g CERTs in Europe: The mechanism offers value to CERTs by providing good practices for developing baseline capabilities necessary for n/g CERTs. It also provides further guidance to EU Member States in adhering to the communications and recommendations (relating to CERTs and their baseline capabilities) of the EU Commission and other EU institutions.
IETF: RFC-2350 (2003 updated)	Same format used: The mechanism provides value by being a widely used and accepted good practice guide for CERTs.
TF-CSIRT/TI: 'Accreditation'	Trust and recognition within the European CERT community: The mechanism provides confirmation of CERTs' capabilities when they are approved for accredited status, along with certain other benefits such as information sharing between CERTs which have reached this level.
FIRST: 'Full Membership'	Trust and recognition within the global CERT community: The mechanism provides confirmation of CERTs' capabilities. In addition, the mechanism provides what it terms 'value added services', including access to good practice documents, technical colloquia, classes, an annual incident response conference, as well as various publications.
APCERT: 'Membership'	Trust and recognition within the Asia-Pacific CERT community: The mechanism provides confirmation of CERTs' status, as well as certain value-added services such as an annual drill test[56] for members, efforts to increase information sharing among members, and joint research and development efforts.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	Following the same practices globally: This mechanism provides value through good practices to its target audience.

4.2.6 Definitions and terminology

For this tier we go one step further and shift focus from definitions of basic terms like 'CERT' and 'constituency' to categories of capabilities and incident classification and definition. ENISA and TF-CSIRT/TI have relatively similar definitions of 'incident' – definitions that focus on incidents' impact on computers and networks. Under their mechanisms, the definition is the baseline evaluation for

[56] For information on the 2013 drill test see: http://www.hkpc.org/index.php?option=com_content&view=article&id=4291%3Ados&catid=149%3Anews-flash&Itemid=437&lang=en

whether something qualifies as an incident.[57] FIRST's definition of incident is more thorough but still maintains the focus on computers and networks: 'An event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information.'[58] IETF and CERT/CC also specify various types of incidents.

On the other hand, there are significant differences among definitions concerning the categories of CERT capabilities. While ENISA provides its set of four baseline capabilities, the other mechanisms, although mostly covering the same topics, have their capabilities/topics scattered in more categories under different headings. The difference is most striking when compared with membership mechanisms like those of FIRST and APCERT. ENISA also pays significant attention to mandate and strategy issues, which do not feature that prominently in the case of other mechanisms. On the other hand, these more often address added value of the CERTs like the benefits of the teams for the wider CERT community (member application process at APCERT where a CERT has to demonstrate benefits it brings to APCERT).

Tier 2 Mechanism	Definitions and terminology	
	Categories of capabilities	**Incident – definition and classification**
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012)	Four baseline capabilities are defined for n/g CERTs: • mandate & strategy • service portfolio • operation • cooperation	The term 'incident' is not specifically defined but the focus is clearly on incidents affecting critical information infrastructure.
IETF: RFC-2350 (2003 updated)	The following categories are listed: • Charter (mission statement, constituency, sponsorship/ affiliation, authority) • Policies (incident types and support levels, cooperation, interaction and disclosure of information, communication and authentication) • Services (incident response, proactive activities)	Computer Security Incident: 'any adverse event which compromises some aspect of computer or network security.' The following categories are mentioned: • Loss of confidentiality of information • Compromise of integrity of information • Denial of service • Misuse of service • Damage to the systems
TF-CSIRT/TI: 'Accreditation'	Categories used when applying for the 'Accredited' status: • constituency	The mechanism includes references to other sources, especially RFC-2350.

Tier 2 Mechanism	Definitions and terminology	
	Categories of capabilities	**Incident – definition and classification**
	• business hours • policies • membership of professional team/ security organisation • services provided to the constituency	
FIRST: 'Full Membership'	The current application form includes (inter alia) the following categories: • constituency • services • business hours • additional (incl. networks of expertise)	*Incident*: 'an event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.'
APCERT: 'Membership'	The membership process includes (inter alia) the following categories: • constituency • host organisation • authority (to act as a CERT) • technical and managerial skill-set of the team • mission statement • trust • contribution to security community	The mechanism does not have its own definitions of incidents but uses the term 'Type of incidents and level of support' introduced by RFC 2350.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	This mechanism applies the following categories: • CSIRT framework (constituency, place in organisation, relationship to other teams) • CSIRT services • Policies (implementation, maintenance and enforcement) • Team operations	Although this mechanism is very detailed on various aspects of incident handling service, the actual definition of an incident is not included. It is, however, present in other CERT/CC documents, including its FAQ section on its website[59]: 'Any real or suspected adverse event in relation to the security of computer systems or computer networks' or 'The act of violating an explicit or implied security policy'.

[59] http://www.cert.org/csirts/csirt_faq.html#2

Tier 2 Mechanism	Definitions and terminology	
	Categories of capabilities	**Incident – definition and classification**
		It also lists some categories of incidents: • attempts (either failed or successful) to gain unauthorised access to a system or its data • unwanted disruption or denial of service • unauthorised use of a system for the processing or storage of data • changes to system hardware, firmware or software characteristics without the owner's knowledge, instruction or consent

4.2.7 Keeping the mechanism up to date

Membership organisations seem to have more explicitly stated routes for updating their mechanisms than non-membership organisations. For example, FIRST's framework can be amended with a two-thirds vote of members present at a General Meeting or Special or Additional Meeting, provided a quorum is present.[60] Meanwhile, APCERT's members can propose additions and changes to policies and procedures by submitting the proposed changes in writing to the Steering Committee, along with the reason for the proposed change. The Steering Committee then decides whether to accept, reject or amend the proposal, and submits it as necessary to Operational Members, which must approve it by at least a two-thirds vote of a quorum during a general meeting, or by more than half of total members if done by email.[61]

Tier 2 Mechanism	Keeping the mechanism up to date
ENISA: *Baseline Capabilities for National / Governmental CERTs* (2010, 2012) – policy recommendations	This is a living document that was updated in 2012, while further updates will follow taking account of the evolving cyber-security landscape and the role of n/g CERTs in the EU Member States with regard to the EU policy scope.[62]
IETF: RFC-2350 (2003 updated)	The mechanism does not explicitly provide for keeping it updated.
TF-CSIRT/TI: 'Accreditation'	The mechanism does not explicitly provide for keeping it updated.
FIRST: 'Full Membership'	The mechanism allows for amendment of its framework with a

[60] http://www.first.org/about/policies/op-framework#c12, under Amendments

[61] AP-CERT Operational Framework, available at http://www.apcert.org/documents/pdf/OPFW_26March2013.pdf

[62] See the recent EU Cyber Security Strategy and the proposal for a Directive on Network and Information Security: http://www.eeas.europa.eu/policies/eu-cyber-security/

	two-thirds vote of the members present at a General Meeting or with a quorum at a Special or Additional Meeting.
APCERT: 'Membership'	The mechanism allows its members to propose additions or changes to policies and procedures by submitting the proposed changes to the Steering Committee, which then decides whether to accept, reject, or amend it.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	This mechanism does not make specific provisions for keeping it up to date.

4.2.8 Promoting the mechanism and CERTs' training

ENISA has gained credit especially among the n/g CERT community thanks to its extensive training material[63] and its dedicated operational events. ENISA CERT Exercises and training material were introduced in 2008. Four years later, new training scenarios were added (bringing their total to 23) containing essential and advanced materials for CERTs in the area of cyber-security. The material includes handbooks for teachers, toolsets for students and also virtual images to support hands-on training sessions. Since 2005, ENISA has also been organising annual CERT workshops for n/g CERTs focusing on the actual needs of the teams including hands-on technical sessions.[64]

ENISA recently introduced its training courses for CERTs in the EU Member States. This is a new initiative to promote and support CERT maturity in the MS by providing exercises and technical hands-on training on different services, operations and cooperation in the daily work of the teams.[65]

FIRST and TF-CSIRT/TI do not engage in significant promotion of their mechanisms, and nor does APCERT. FIRST has a formal policy for engaging with the press. APCERT issues media releases relating to its key activities.

By tradition the first TF-CSIRT/TI meeting each year is co-organised with FIRST to safe travel budget for all participants and to raise value added. Similarly ENISA usually co-locates its annual CERT workshop[66] with the second TF-CSIRT/TI meeting. Additionally, FIRST offers two technical colloquia[67] each year that last from half a day to 2 days and are often conducted in cooperation with a local CERT member. FIRST also offers a regular annual conference/ general meeting[68] to its members, which are valuable for both Tier 1 and Tier 2 CERTs aiming to further develop their capabilities. As mentioned previously, TF-CSIRT/TI offers a training programme under this Tier which is TRANSITS II (advanced training).[69] APCERT does not offer its own training programmes, but does provide a list of meetings and training opportunities available in the Asia-Pacific region offered by its member CERTs and other relevant organisations.

[63] http://www.enisa.europa.eu/activities/cert/support/exercise
[64] http://www.enisa.europa.eu/activities/cert/events/past-events
[65] http://www.enisa.europa.eu/activities/cert/support/exercise
[66] http://www.enisa.europa.eu/activities/cert/events/past-events
[67] http://www.first.org/events/colloquia
[68] http://www.first.org/events/agm
[69] http://www.terena.org/activities/transits/transits-ii/

Tier 2 Mechanism	Promoting the mechanism and CERTs' training
ENISA: *Baseline Capabilities for National / Governmental CERTs – Policy recommendations* (2010, 2012)	ENISA provides n/g CERTs with extensive training material and also organises workshops and tailored training courses, often focused on technical issues as requested by the teams.
IETF: RFC-2350 (2003 updated)	The mechanism does not make specific provisions for its promotion or provisions related to training.
TF-CSIRT/TI: 'Accreditation'	There are regular meetings held three times a year and TF-CSIRT/TI promotes training programmes like TRANSIT-II.
FIRST: 'Full Membership'	The mechanism offers two technical colloquia each year that last from half a day to 2 days and are often conducted in cooperation with a local CERT member, as well as a regular annual conference/ general meeting. Based on the agreement with TERENA (TF-CSIRT/TI), FIRST also offers TRANSIT courses.
APCERT: 'Membership'	The mechanism does not offer its own training programmes, but does provide a list of meetings and training opportunities available.
CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)	This mechanism does not make provisions for its promotion or provisions related to training.

4.3 Tier 3 of the CERT Maturity Model

CERTs that have reached Tier 3 of the CERT Maturity Model have established themselves and are well balanced in their daily work and experience. They have a complete set of capabilities (all well documented) in place and a stable position within their community, meaning that they no longer depend on individuals from their team. Thus, for CERTs that have reached this level, CERT mechanisms can be helpful in terms of refining their capabilities and establishing recognition of the extent to which they have developed their capabilities. They can also provide feedback to CERTs and the cyber-security communities to improve the work of CERTs based on their extensive and proven knowledge, experience and recognition.

There are fewer mechanisms targeting CERTs that have reached this level, but several organisations have standards and mechanisms that can be recognised as being appropriate for Tier 3 CERTs:

1. ENISA: n/g CERT standard capabilities (2014)[70]
2. ISO: ISO 27035 (2011)
3. TF-CSIRT/TI: Certified status

[70] This project on n/g CERTs standardised capabilities is ongoing (beginning in 2009) with next input due in 2014.

4.3.1 Type of approach (organisation)

Gaining 'certified' status with TF-CSIRT/TI is the next step beyond accreditation for member CERTs. The International Standards Organisation (ISO) is a non-governmental organisation that is made up of members from the national standards bodies of 163 countries.

The ISO-27035 document, like the other ISO standards that it publishes, was developed by a panel of experts on a technical committee. Thus, it is a consensus-based document, even though ISO itself is not a membership organisation for CERTs in the same way that TF-CSIRT/TI or FIRST are. Therefore, as for Tier 1 and Tier 2 CERTs, the organisations with mechanisms for Tier 3 CERTs follow different organisational approaches.

ENISA is also aiming to contribute with its mechanism to Tier 3 of the CERT Maturity Model while building on its earlier work in defining and deploying baseline capabilities for n/g CERTs. This project on n/g CERTs standardised capabilities is ongoing, with next input due in 2014.

Tier 3 Mechanism	Type of approach (organisation)	Voluntary/ subscribe/ compulsory form
ENISA: *n/g CERT Standard Capabilities* (2014)	According to the new ENISA mandate (EU Regulation 526/2013)[71] ENISA will assist CERTs in advancing their capabilities so that they increasingly correspond to those of the most developed CERTs. For this purpose ENISA should promote the establishment and operation of a peer review system.	compulsory (once joined)
ISO: *ISO 27035* (2011)	The mechanism was developed by a panel of experts of a committee and is therefore a consensus-based standard, not a membership-driven mechanism.	compulsory (once joined)
TF-CSIRT/TI: 'Certification'	This mechanism is formal and membership-based, with formalised processes for accepting members and internal processes.	compulsory (once joined)

4.3.2 Requirements for CERTs

TF-CSIRT/TI provides CERTs that have already earned accredited status with it the opportunity to apply for certification, which is meant for teams with 'internal and/or external reasons to have their maturity level gauged in an independent way'. To apply for certified status, a CERT must be accredited by TF-CSIRT/TI, be in good standing with the organisation for at least eight months, not be under special review by the TF-CSIRT/TI Review Board, and must have attended at least one TI Accredited Team meeting.[72] The requirements for ISO compliance are straightforward.

[71] http://www.enisa.europa.eu/about-enisa/regulatory-framework
[72] http://www.trusted-introducer.org/processes/certification.html

Tier 3 Mechanism	Requirements for CERTs
ENISA: *n/g CERT Standard Capabilities* (2014)	Not yet defined[73]
ISO: *ISO 27035* (2011)	The requirements result from the compulsory set of standards once a CERT decides to follow them.
TF-CSIRT/TI: 'Certification'	Defined: The mechanism requires applicants for 'Certification' already be accredited by TI, be in good standing with the organisation for at least eight months, not be under special review by the TI Review Board, and must have attended at least one TI Accredited Team meeting.[74] Certification is valid for three years, after which a re-certification process must be started and passed in order to keep the 'certified' status.

4.3.3 Validation process

TF-CSIRT/TI uses the Security Incident Management Model (SIM3 Model)[75] as a basis for evaluating a member's application for certification. The SIM3 Model is similar to the ENISA baseline capabilities in terms of how the model is organised, with key areas of focus being organisation, human resources, processes, and tools. Each CERT capability is evaluated using a five-point scale, ranging from '0', which means it is not available, to '4', which means that the capability is not only described (on level '2') and rubber-stamped (on level '3') but also part of an audit process. According to TF-CSIRT/TI, the certification process takes between three and twelve months in total.[76]

In case of ISO standards independent audits are used for the validation of the implemented standard.[77] ISO provides good practices for choosing an auditing company.

Tier 3 Mechanism	Validation process
ENISA: *n/g CERT Standard Capabilities* (2014)	Not yet defined.[78]
ISO: *ISO 27035* (2011)	Independent audits are carried out.
TF-CSIRT/TI: 'Certification'	Minimum score needs to be attained for each criteria in the SIM3 model. The minimum scores are defined by the TF-CSIRT Steering Committee.

[73] This project on n/g CERTs standardised capabilities is ongoing with next input due in 2014
[74] http://www.trusted-introducer.org/processes/certification.html
[75] http://www.trusted-introducer.org/SIM3-mkXV-TI.pdf
[76] http://www.trusted-introducer.org/processes/certification.html
[77] For an example of independent auditing services for ISO 27035 see http://www.isec.ro/compliance/iso-iec-27035-incident-management.
[78] This project on n/g CERTs standardised capabilities is ongoing with next input due in 2014.

4.3.4 CERTs' focus: Type and region

The same geographic and sector-specific focuses of the CERT community organisations relevant for Tier 3 CERTs apply as previously discussed in this document. ENISA and TF-CSIRT/TI are focused on Europe, while ISO seeks to provide value to CERTs worldwide. ENISA's mechanism specifically focuses on n/g CERT sector-specific group in EU Member States.

Tier 3 Mechanism	CERTs' focus: type and region
ENISA: *n/g CERT Standard Capabilities* (2014)	n/g CERTs/EU Member States[79]
ISO: *ISO 27035* (2011)	all types of CERTs/global
TF-CSIRT/TI: 'Certification'	all types of CERTs/Europe

4.3.5 Benefits and added value of the mechanism

Under Tier 3 the main benefit for the teams should be: the recognition by wider CERT and cyber-security community of the team capabilities (by attaining a 'quality mark'). The added value should be facilitating cooperation with institutions regarding standard operational procedures, financing and grants.

Reaching the level of certification with TF-CSIRT/TI serves as independent affirmation of a CERT's capabilities, which it can use with its constituents, its funding bodies, and with other parties or teams. Thus, the value of reaching the level of Certified with TF-CSIRT/TI revolves around a CERT's ability to use TF-CSIRT/TI's judgment to demonstrate its capabilities with its most important partners – namely its constituents and funding sources.

The International Standards Organisation offers a different type of value to CERTs. ISO goes beyond providing good practices to offering internationally agreed-upon standards for CERTs to follow. This is potentially quite valuable both in terms of helping a CERT build up and maintain its capabilities, as well as in terms of supporting a CERT's arguments for why it needs funding or resources for developing certain capabilities.

Tier 3 Mechanism	Benefits and added value
ENISA: *n/g CERT Standard Capabilities* (2014)	This mechanism will provide a wide range of benefits[80], including access to good practices and networking with CERTs offering these good practices. Another added value is formal recognition by EU authorities and an independent (and expert) affirmation of the team's capabilities.
ISO: *ISO 27035* (2011)	The mechanism provides value by being an accepted good practice guide for CERTs based on a specific standard.
TF-CSIRT/TI: 'Certification'	The mechanism serves as independent affirmation of a CERT's capabilities, which it can use with its constituents, its funding bodies, and with other parties or teams. The certification may be

[79] This project on n/g CERTs standardised capabilities is ongoing with next input due in 2014.
[80] This project on n/g CERTs standardised capabilities is ongoing with next input due in 2014.

	regarded as a kind of 'extra branding' that is useful for many purposes in the team's future.[81]

4.3.6 Definitions and terminology

For Tier 3 mechanisms that are suitable for advanced CERTs it is useful to consider standard services (core or 'must have' services), working regime and incident response time. While TF-CSIRT/TI 'Certified status' is based on the above-mentioned SIM3 model, the other two mechanisms are either being developed (ENISA's baseline capabilities mechanism) or being reviewed (ISO 27035). But they will probably not change much in their approaches. Therefore, a similar approach can be expected: incident handling (and incident management in general) will be considered as a core service that a CERT offers to its constituents, one that provides 24/7 reachability mode and fast response timelines based on the severity of the incident.

Tier 3 Mechanism	Definitions and terminology		
	Standard services (core/ must have services)	**Working regime (for core/ must have services)**	**Incident response time**
ENISA: *n/g CERT Standard Capabilities* (2014)	Incident handling Alerts and warnings Announcements	24/7	yet to be defined
ISO: *ISO 27035* (2011)	Handling an incident that 'has a severe impact on the organisation's core services, instigating "crisis" activities through escalation to the Crisis Team.'	24/7	'If an organisation contracts with an external party for support, for example a CERT, then it should be ensured that all requirements, including response times, are included in the contract with the external party.'
TF-CSIRT/TI: 'Certification'	This process requires the description of services provided and level of support (speed of reaction to incoming incident reports from constituents and from peer CERTs)	24/7	Minimum requirement: 'Specifies the speed of reaction to incoming incident reports and reports from

[81] At the time of writing this document only seven teams had successfully completed the accreditation process: http://www.trusted-introducer.org/directory/alpha_certification_Z.html (last accessed on 20 September 2013)

			constituents and from peer CERTs. For the latter a human reaction within two working days is the minimum expected.'

4.3.7 Keeping the mechanism up to date

ISO appears to follow an iterative process whereby the panel of experts responsible for a particular set of standards updates those standards as necessary. ISO's work on CERTs is a relatively small part of its overall activities, so the process for keeping its CERT mechanism updated is less explicit than with other organisations that have a greater focus on CERTs.

The SIM3 model that is the basis for TF-CSIRT/TI's certification process has no explicit provision as to how it can be updated, although updates to this model would be necessary for TF-CSIRT/TI if it were to decide to make fundamental changes to its certification process.[82]

Tier 3 Mechanism	Keeping the mechanism up to date
ENISA: *n/g CERT Standard Capabilities* (2014)	Not defined yet.[83]
ISO: *ISO 27035* (2011)	The mechanism probably follows an iterative process whereby a panel of experts revisits their standards, although the process for keeping this particular standard up to date is not explicitly stated. There was an ongoing revision of the standard at the time of writing of this document.
TF-CSIRT/TI: 'Certification'	The updates are the responsibility of the TF-CSIRT Steering Committee. Big changes require a vote by the members (TF-CSIRT Full Members).

4.3.8 Promoting the mechanism and CERTs' training

ISO is not heavily engaged in promoting its standards, although it does actively promote the participation of new players in the process of creating relevant standards. ISO offers a variety of training courses designed 'for individuals performing various roles in International Standardization' and 'offered to all ISO members'. It notes that these training courses help members with regard to specific aspects of the development of ISO standards as well as with distributing and implementing the standards.[84]

[82] SIM3: Security Incident Management Model *(2010),* available at https://www.trusted-introducer.org/SIM3-mkXV-TI.pdf
[83] This project on n/g CERTs standardised capabilities is ongoing with next input due in 2014.
[84] http://www.iso.org/iso/home/about/training-technical-assistance.htm

TF-CSIRT/TI does not offer specific training courses to certified members. The SIM3 Model considers staff training to be one of the fundamental aspects of the 'Human' Parameters of the model, although it does not make specific recommendations with regard to training programmes.[85] ENISA has developed its advanced tailored training suitable also for teams in Tier 3 level.[86]

Tier 3 Mechanism	Promoting the mechanism and CERTs' training
ENISA: *n/g CERT Standard Capabilities* (2014)	ENISA provides n/g CERTs with extensive training material and also organises specific workshops, often focused on technical issues as requested by the teams or dedicated to a particular area (e.g. CERT and LEA cooperation on cybercrime).[87]
ISO: *ISO 27035* (2011)	The mechanism does not make specific provisions for its promotion or about training, but it does promote the participation of new actors in the creation or revision of standards.
TF-CSIRT/TI: 'Certification'	The TRANSITS-II courses are intended for more experienced personnel working for established CERTs. They provide insights into key areas in incident handling and response operations, training in how to improve communications with constituents, as well as practical exercises.[88]

[85] SIM3: Security Incident Management Model (2010), available at https://www.trusted-introducer.org/SIM3-mkXV-TI.pdf
[86] http://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii
[87] http://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii
[88] http://www.terena.org/activities/transits/transits-ii/

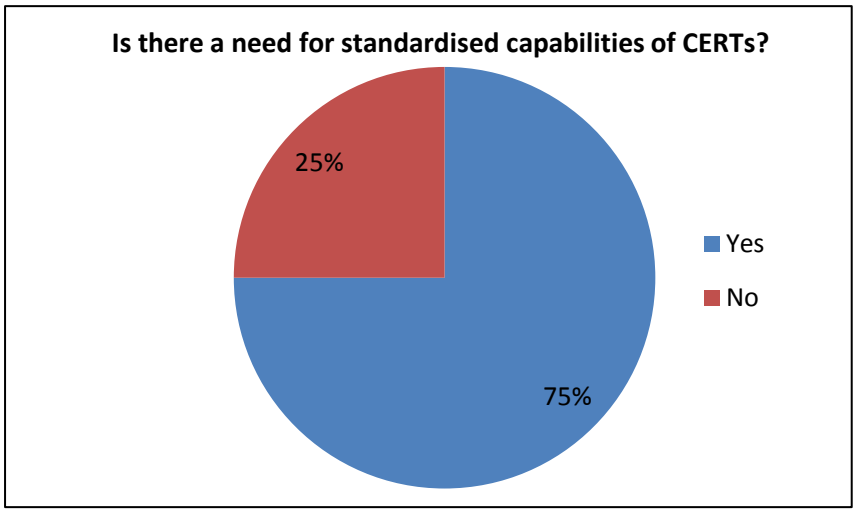
5 Harmonisation Approach

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

That said, there will be parts of all of these mechanisms that either will be very unlikely to be considered for harmonisation or would not benefit from efforts to harmonise. These organisations and their mechanisms serve different purposes and have different objectives, meaning that harmonisation will not be possible across all, or even most, areas. The objective of this section is to identify some areas where ENISA believes that harmonisation efforts could potentially be beneficial, and also to identify areas where harmonisation efforts are unlikely to be fruitful.

5.1 Interest in harmonisation

Most surveyed CERTs say that they see a need for CERTs to have standardised capabilities. The CERTs are also of the opinion that harmonisation in some areas of CERT mechanisms discussed below could potentially benefit them (and their constituents!) in terms of reaching the goal of standardised CERT capabilities.



Number of answers = 12 n/g CERTs

Source: Survey conducted by ENISA in conjunction with this document

CERTs' interest in standardisation of capabilities suggests that CERT community organisations should give thought to where harmonisation might be beneficial in their mechanisms. This will be the foundation for efforts to harmonise specific capability areas going forward. These organisations know that their mechanisms can potentially benefit from harmonisation: for example, FIRST already

has a liaison relationship with ISO through which standardisation efforts are made.[89] ENISA and TERENA cooperate on TRANSITS courses, for which ENISA provides financial and content-related support.

5.2 Suitable areas for harmonisation

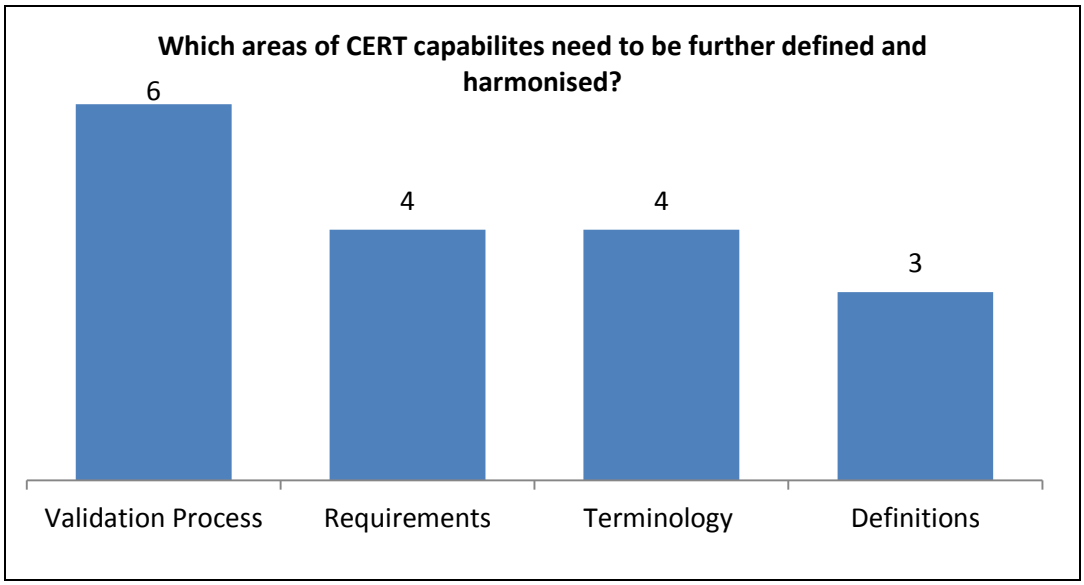
Surveyed CERTs see the most potential in harmonisation for the areas of (1) accepting and validating members and (2) terminology and definitions. This is an interesting result because these are very different aspects of the considered mechanisms and raise unique challenges in possible efforts to harmonise them.

(1) ***Requirements / Validation Process***: The CERT community's interest in harmonisation when it comes to mechanisms' requirements and validation processes is understandable because meeting and then adhering to different requirements is resource- and time-intensive. Harmonisation of requirements seems to be more straightforward: CERTs already use the same tools/equipment or way of communication (e.g. PGP encryption, phone number for incident reporting, web-based incident report form, participation in the community meetings, etc.).

From the perspective of CERTs, it would be better if they could meet a single validation process regardless of the CERT organisation from which they are seeking validation. Harmonisation is likely to be challenging to achieve in these areas, though: CERT organisations have different missions and agendas, and they may be reluctant to give up the autonomy that comes with having their own requirements and validation processes.

(2) ***Definitions / Terminology:*** Working to harmonise important terms and definitions across mechanisms is likely to be a more realistic goal than validation processes or requirements. Many terms and definitions used by CERT organisations are already similar, as discussed previously in this document. Thus, beginning the process for harmonising concepts at the core of CERTs' capabilities and responsibilities might be the right place to begin harmonisation efforts. Harmonising core terms such as: CERT and constituency definitions in Tier 1, incident type and definition for Tier 2 and incident response time for Tier 3 CERTs would seem to make considerable sense. This could be a way to make these mechanisms fundamentally more compatible and make it easier for CERTs to belong to or utilise more mechanisms and also for CERTs' constituency and cooperation partners to understand better and recognise teams' capabilities.

[89] http://www.first.org/global/standardisation



Number of answers =12

Source: Survey conducted by ENISA in conjunction with this document

A number of other areas may be particularly conducive to capability harmonisation efforts:

- CERT types and the sectors in which they operate: The harmonisation of definitions of sectors on which vertical-specific CERTs typically focus may be beneficial, as this would offer more clarity and transparency surrounding a CERT's activities and the constituents it serves.

- Training: This is another area where harmonisation could be beneficial, as it could lead to synergies, proliferation of training opportunities for CERTs (in terms of standardised capabilities and services offered by CERTs), and more opportunities for CERTs to meet and share good practices. Good progress has already taken place in this respect with several CERT organisations (including ENISA and FIRST) supporting TERENA's TRANSITS training for CERTs.

On the other hand, harmonisation will be more challenging or makes less sense for some other areas of capability mechanisms:

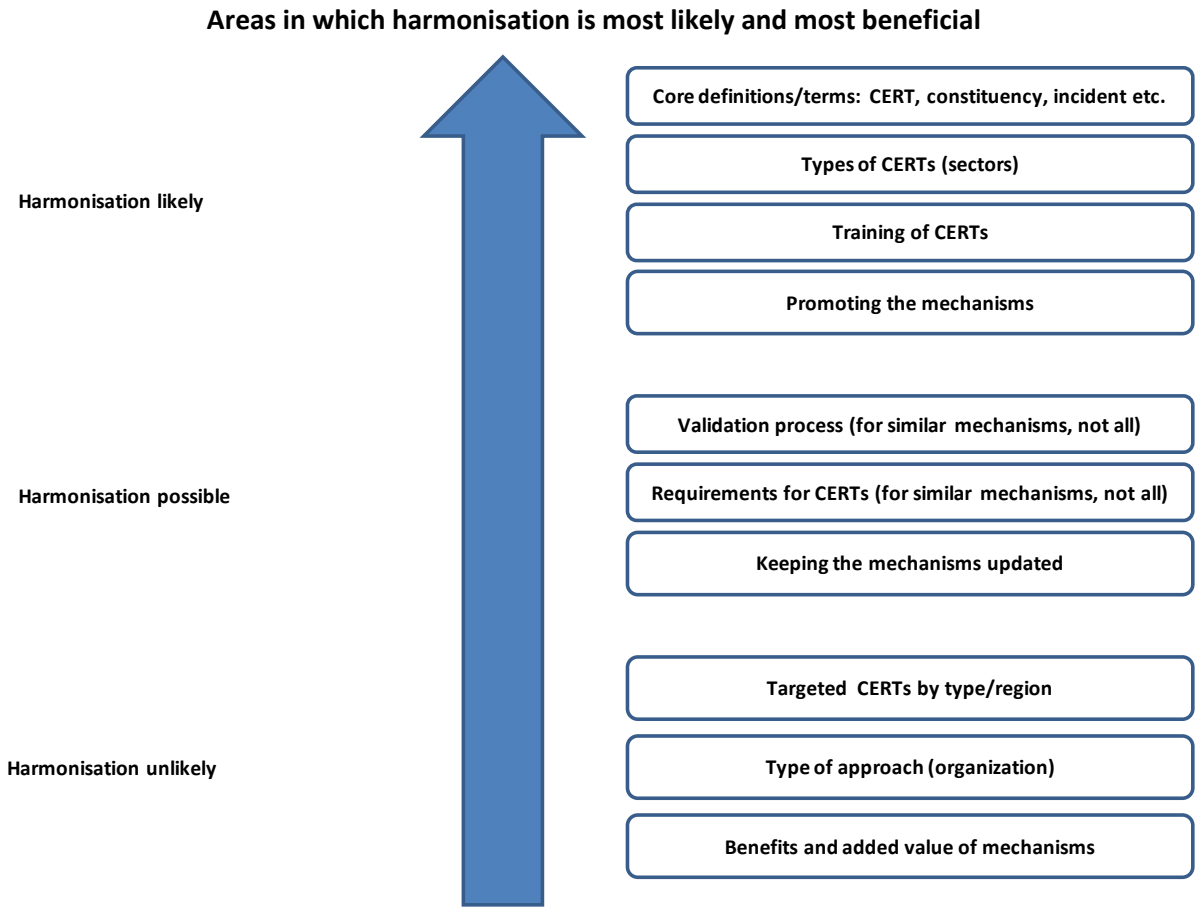
- Approach (type of organisation): This is fundamental to a mechanism and approaches differ to such an extent that harmonisation will be challenging.

- Benefits: The benefits that CERTs can gain from an organisation's capability mechanism are unlikely to merge to an appreciable extent as benefits are fundamental to an organisation's identity.

- Promoting the mechanisms: Organisations will continue to pursue different strategies when it comes to promoting their mechanisms.

The figure below provides a view of the areas in which these organisations are most likely to be receptive to the potential of harmonisation. As discussed, areas such as definitions of core

terminology will rank among the areas most likely to see harmonisation, whereas harmonisation will be looked at more sceptically when it comes to areas that go to the core of what the organisation does.



Next steps

Actions to be taken by organisations offering their CERT mechanism:

- *Address the suitable harmonisation areas*

It is desirable to start discussions among CERT organisations on the usefulness of harmonisation of certain areas of their CERT capability mechanisms, especially as regards the requirements for a CERT to join a particular CERT organisation or its CERT capability mechanism.

- *Agree on a list of areas to be harmonised*

The discussion among various CERT organisations should identify areas considered as suitable for harmonisation. It is suggested that the primary harmonisation focus should be on definitions of basic terms, which would support interlinks among the CERT organisations and be helpful for teams that are members of several CERT organisations.

Actions to be taken by ENISA

- *Address the missing criteria in the maturity assessment for its n/g CERT standard capabilities mechanism*

ENISA's n/g CERT standard capabilities mechanism will be adjusted based on the interaction with the teams. The focus will be on updating the list of maturity assessment criteria by adding new items and possibly deleting others if they are found no longer relevant.

- *In collaboration with EU Member States continue to support the established n/g CERTs*

It is necessary that the CERTs further develop their capabilities so that they are in a position to rise up the maturity scale. This is important for fulfilling the objectives of new EU Cyber Security Strategy. ENISA will support the teams with new training materials.

- *Further monitor the deployment of baseline capabilities of n/g CERTs in EU Member States as well as developments in other CERT organisations in this area*

ENISA will continue its stocktaking efforts in the area of baseline capabilities. At the same time it will monitor the developments in other CERT organisations as regards their CERT mechanisms.

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

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

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