Stelvio

www.Stelvio.nl

The Trusted Introducer service:

Fostering cooperation and trust between CSIRTs in Europe (and beyond) by establishing & maintaining a trusted repository of well-modelled CSIRT service information.

http://www.ti.terena.nl
ti@stelvio.nl

The Trusted Introducer Team:

Mark Koek
Erwan Smits
Don Stikvoort
Klaus-Peter Kossakowski

Stelvio
Amersfoort, The Netherlands

May 1st, 2001

1 Roadmap

Of course you want to read all of this article. In that case just process it serially, and you will get to know about purpose, background and operations of the Trusted Introducer (TI).

Perhaps though, you have to spare some time, but still want to understand what TI is about and how it operates. In that case, skip the background chapters and only read chapters 2, 6 and 7 (and probably also 8, the management summary), and have a short peek at Appendix B. They are all in 12 pitch font, whereas the background information is in 11 pitch font.

If you just want the management overview – read chapters 2 and 8 only. Then you will approximately know what TI does – but not have much of a clue about why and how. It is up to you.

2 Introduction

The mission statement of the so-called Trusted Introducer service is as follows:

The Trusted Introducer must foster trust and cooperation between *CSIRTs in Europe, both new and experienced. The vehicle used to achieve this is to invite CSIRTs to present themselves and describe their service according to an established baseline – thus enabling objectivity, which is regarded as the pre-requisite of trust.*

The Trusted Introducer service is operational in a pilot setting as of September 1st 2000. Prime enabler is the TERENA association [1], which has played an active role in fostering cooperation between CSIRTs of all kinds inside Europe since 1992. The Trusted Introducer contract was won by Stelvio of Amersfoort, The Netherlands [2]: "we" in this report stands for the Trusted Introducer team at Stelvio.

This report will introduce the Trusted Introducer service, by exploring the considerations of early 2000 that led to the actual Trusted Introducer set-up on September 1st of the same year. The analysis that took place early 2000 by the way has lost nothing of its actuality, reason to present it here in an only slightly abridged version.

The original starting point was to describe a process of introduction and accreditation of new CSIRTs - in order to bring them into "the web of trust" – and to set criteria to foster the objectivity and authenticity of such a process. At the same time it was recognized that this "web of trust" had to be maintained henceforth based on the same accreditation criteria.

A pragmatical limitation to European CSIRTs was introduced because of the European scope of the funding body, TERENA. However, it was recognized from day one that good international cooperation beyond Europe was essential for the accreditation process to succeed on the longer run.

[1] TERENA (Trans-European Research and Education Networking Association), see http://www.terena.nl.

[2] Stelvio, independent consultants in Internet Technology and Security, see http://www.stelvio.nl .

3 Early 2000 considerations (i) -- Definition of CSIRT

To avoid fuzzyness we raise the question: what **is** a CSIRT anyway?

[RFC 2350] has a good implicit definition:
“Any group calling itself a CSIRT {or CERT or IRT or …} for a specific constituency must therefore react to reported security incidents [3], and to threats to "their" constituency [4] in ways which the specific community agrees to be in its general interest.”

However, “react to {…} incidents” is pretty open, so we need [West-Brown et al. 1998] to narrow that down:
“{CSIRT:} A team that provides a basic set of services (contact point for reports, support when incidents occur and feedback in regard to requests addressed to the team). Announcement services might also be offered as well as other services as defined by the team. The team might serve different constituencies, and might even provide different service packages or service levels.”

The combination of both statements gives a good enough picture of what we conceive a CSIRT to be. Most probably e.g. all serious ISPs entertain CSIRTs – even if they do not use such a label explicitly, because:

If an entity A entertains a FUNCTION B where customers/constituencies can report computer/network security incidents, and B then handles these reports in a constructive and secure way (consultancy, coordination, feedback, …), then function B essentially is the CSIRT of entity A.

The above definition of a CSIRT does not prescribe coordination with other CSIRTs as a necessary task. A CSIRT could in theory be an island, but clearly for the goal of this report such teams are not of interest. In fact such teams deny their constituency potential benefits arising from information exchange, expertise of other teams and supportive information from sites external to the constituency but involved in an incident. Thus:

Interaction between teams on specific incidents, i.e. the task of incident coordination, is an explicit part of the CSIRT definition in this report.

[3] Incident [West-Brown et al. 1998]: any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of such events are:
- Intrusion of computer systems via the network (often referred to as "hacking");
- Occurences of system anomalies like computer viruses;
- Probes for vulnerabilities via network connections to a range of computer systems (often referred to as "scans").

[4] Constituency [West-Brown et al. 1998]: a specific group of people and/or organizations that have access to specific services offered by a CSIRT.

4 Early 2000 considerations (ii) -- Situation Report

Organisations slowly build up an incident response capability. The following phases can be separated:

I. Non-recognition: the problem is not recognized, all handling of security problems is done within the line organisations, no coordination to the outside other than per chance. Most organisations inside Europe still are in this phase, and even many ISPs. The US is a few years ahead of Europe: the awareness of the problem is becoming more widespread in organisations of medium and bigger size.

II. De-facto incident management: the problem is recognized, maybe an instance to report to is installed internally, but no structural effort inside, nor stuctural links to the outside. In the coming few years the majority of medium sized and bigger organisations inside Europe will grow into this phase.

III. Structured incident management: an incident response capability – let's name it a CSIRT – is available, and is linked to other CSIRTs in the world. Typically these teams are (striving to become) FIRST members, or associated with or customer of a FIRST member. Phase III could be separated into two subphases:
   a. Not yet part of the web-of-trust
   b. Part of the web-of-trust

The approximately 100 teams worldwide that are members of FIRST are mainly in phase III, several tens of them in IIIb: FIRST membership alone is not enough to become part of the web-of-trust, though it helps significantly – but also active participation in the community is needed, say: visibility. One other factor is important also: continuity. If a team cannot uphold its quality (by, for example, distributing wrong or incomplete information), trust can evaporate.

What then is this elusive web-of-trust that pops up in this report? A definition by example is the best clarification. A team is inside the web-of-trust if it is able to report an incident to another team also inside that web-of-trust and to be taken seriously at once, trusted that the information provided is correct, and be helped with some priority (over average reports). Information from teams inside the web-of-trust are more strongly considered as other information, as the other teams trust the team to know the background of incident response, make realistic assumptions and assessment due to their knowledge [5]. *Also note that the web-of-trust is not*

[5] In the early nineties to become part of the web-of-trust it was essential to go e.g. to a FIRST conference and „drink beer in a pub with the right people" – however useful and enjoyable this still may be, it is not enough anymore, the CSIRT society has become too big, people change places too often, and the financial stakes involved in network security have become too high.

necessarily a singular entity with an any-to-any characteristic: there is more than one trust-circle, and those circles meet at some places (i.e. CSIRTs).

TERENA members – European NRENs [6] - will typically be in phases II-III. Especially those in phases II and IIIa – the majority we presume - are of course of interest to this report, since for those there is work to be done: the gradual transformation to phase IIIb.

A breakdown of current FIRST members within Europe shows 27 teams (status: January 2000), one third of them affiliated with TERENA due to their constituency and/or parent organization:

- 10 Commercial organizations (1 Danmark, 1 France, 3 Germany, 1 Netherlands, 2 Switzerland, 2 UK)
- 9 research and educational networks (1 Danmark, 1 Germany, 1 Kroatia, 1 Netherlands, 1 Poland, 1 Scandinavia, 1 Switzerland, 2 UK)
- 4 Government teams (1 France, 1 Germany, 2 UK)
- 4 "other" teams (1 Germany, 1 Israel, 1 Italy, 1 UK)

It goes without saying that the above suggested sequence – growing from phases I and II via IIIa to phase IIIb - is the way to go ahead. This is based on the fact that the current cloud of IIIb teams is doing their work moderately well, and –more importantly- that it is ***impossible*** *to keep on doing this work by just expanding the cloud and covering everybody who sends a mail and says: "he, I'm a CSIRT, trust me, send mail". Elusive as "trust" may be, the latter approach is clearly a bridge too far. The trusted cloud must not be expanded, but rather new teams should be drawn into the cloud. The big problem clearly is to retain quality with the cloud becoming denser and denser.*

If we broaden the TERENA perspective – what is exactly what we shall do when defining the scope of CSIRTs in the following chapter - to not only look at TERENA members (mainly research ISPs), but also commercial ISPs, major companies and governmental institutions, plus vendor-product teams and major commercial CSIRTs – all inside Europe - then phases I and II will be pre-dominant. The transition of phase I to II is a gradual one that will take place in the coming few years – the situation in the US is ample proof for that assumption. It needs only background help from national and international initiatives and can thus be fostered by organisations like TERENA, FIRST and established CSIRT teams.

Two important remarks have to be made at this stage. First of all that even being in phase IIIb does not imply that a CSIRT is a fully established entity – the phenomenon is too young for that. "Many CSIRTs in existence today either lack a clear understanding of their goals and objectives or have failed to effectively communicate that information to the parties they interact with" [West-Brown et al. 1998]. As a result, they needlessly expend effort and resources (often in crisis situations) in an attempt to:

[6] NREN : National Research and Education Network.

- understand if they are using the correct priorities to ensure they respond to the most important activity;
- correct any inappropriate expectations of those they interact with;
- understand how and if it is appropriate for them to react to a given situation;
- revise their policies and procedures to meet the needs of the situation;
- determine if the range and nature of the services they offer should be modified.

Until a CSIRT defines, documents, adheres to, and widely distributes a concise and clear mission statement and service definition (as e.g. per [RFC2350]), that situation is unlikely to improve. The consistent lack of time that plagues CSIRTs however does not help the improvement of this situation very much. For the sake of this report we choose to ignore this problem/challenge – we falsely presume here that all that matters is to become part of the web-of-trust. However we shall indirectly contribute to the improvement of this situation by introducing criteria for CSIRTs to meet to help them grow into the web-of-trust: these criteria will be of the useful structural kind (like service definitons) which have been grossly neglected by most old-hand teams because of their pioneering status and lack-of-time[7].

The second important remark is that if we are to define a process that would bring teams from phases II to IIIa and then IIIb, and criteria for teams to meet to help that process along, that also implies that these criteria would be useful to apply to existing IIIb teams. This is far from implying some sort of certification of CSIRTs – time is not ripe for that yet – but it is about an important notion, and that is “trust maintenance”. Now this is a rather new idea in this game. The interesting thing is that it takes years for teams to gain trust, and usually this trust is based for 90% on a few key personal relationships which have been built carefully – and only for 10% on written service or quality statements, site visits and so on. What one sees then is that after the trust has been gained, the key people often move to other places – but magically the trust invested in the team remains – based only on the 10% that is left. This is a potentially dangerous situation, and if only a few things go really wrong, the relationship is wrecked for the years to come. **Trust takes years to gain but is lost overnight.** What would help the situation much is to improve on the 10% part: initially trust is indeed based much upon personal relationships, but once established the structural part (the 10%) should be increased gradually. This again means an emphasis on objective criteria which can be met. And it means that IIIb teams should care about these criteria just as much – probably even more – than IIIa teams, since IIIb teams are much more vulnerable when walking on the waters of trust.

Thus a well defined transfer of phases II to IIIa and IIIb, **and** staying inside the latter phase, the trust-phase, is the topic of this report. It needs saying that gaining entry to the CSIRT community today can be a difficult and lengthy process. The community is ready to embrace new members, but it

[7] Of course several of the old-hand teams have meanwhile corrected the situation and produced service definitions etcetera.

is wary of interacting with new CSIRTs unless an existing member of the trusted community can vouch for them. So some new teams are in a "Catch-22" situation, wanting to contribute, but needing to gain acceptance and mentoring from an existing member of the community before they can begin to gain broader acceptance. As most teams have no charter or funding to act as mentors to new members of the community, finding a mentor and introducer is not as easy a task as it sounds.

Moreover, because there is no formal mentoring process for new members of the community, the guidance given to new teams can vary widely depending on the experiences and time available from their mentoring team. As a result, the CSIRT community expands at a much slower rate than is needed, and the teams operate with a widely varying set of operations and standards. The community needs to ensure and adopt a sponsorship process that doesn't depend on the good will of individual teams and ensures that each team meets an agreed-upon minimum level of operational standards.

In the words of [Kossakowski et al. 1999]:
„Today's approach is not reliable, does not scale, and it must be made more effective. It is critical to have a global response infrastructure to replace a less reliable system based on trust between individuals with a reliable and effective system based on global understanding/agreement."

FIRST could play a much more active role to help establish and maintain such an infrastructure. However, FIRST still being entangled in its change process from an all volunteer effort towards a professional organisation with a distinct set of services funded by its members, it seems reluctant to assume this role. ISOC and IETF are not expected to fill in this gap on the short run either. Therefore especially regional initiatives have a good chance of succeeding. In Europe the research CSIRTs together with TERENA have been in the lead since 1992 and are therefore in an ideal position to achieve inside Europe what FIRST is currently not (yet) undertaking. Good cooperation between TERENA and FIRST would be the best way to avoid precious efforts being spoilt in this area.

This report intends to tackle the afore mentioned problems heads-on: define an objective process (built on criteria) for TERENA to implement as a *trusted introducer* to help organisations evolve from phases II to IIIa and IIIb. A process irrespective of FIRST – though indeed the implementation of such a process postulates a relationship to FIRST and could even be seen as the prelude to a conceivable European chapter of FIRST. In fact, the adoption of the process - once it has shown its success - should be suggested to FIRST. It is expected that TERENA can and should play a leading role here for the next 3 years to come – after that probably a process will take place as we witnessed when the RIPE NCC [8] grew up and

[8] RIPE NCC is the European counterpart of ARIN and APNIC, giving out IP and AS numbers and maintaining the related whois database used for registration and routing purposes. See http://www.ripe.net .

left the parental TERENA house to stand on its own. The comparison is in many ways interesting. However, it is unlikely that the *trusted introducer* will come to stand on its own: it is expected that it will liaise with FIRST or a FIRST follow-up, or with other suitable umbrellas. It is also not very likely that security will become so trivial that the CSIRT system will become useless, nor is it very likely that law enforcement will “take over”: the international cooperation of law enforcement is a daunting problem compared to CSIRT cooperation, and besides, most organisations shy away from relying on law enforcement for the sheer complexity (and cost) that comes with computer forensics and for the fact that they don’t want to see their names in the newspaper – which is a viable risk when a lawsuit takes place.

5 Early 2000 considerations (iii) -- CSIRT Scope

As hinted on above it is useful to state what CSIRTs – or potential CSIRTs - we shall be referring to in this report.

Following the above CSIRT definition, the potential number of teams is clearly a daunting one. There are a few ways to narrow that down. The first one is geographical limitation. TERENA’s geographical constituency is Europe plus neighbouring countries, and this report follows that limitation – though the conclusions of this report would essentially prove valid worldwide as well. Of course incident coordination - and therefore the web of trust - does not stop at the European borders – *It is supposed however in this document that key teams within the European framework do have access “outside”, i.e. to key CSIRTs outside Europe* [9] *, for the sake of incident coordination.*

We could narrow the number of CSIRTs further down by following the TERENA constituency more closely, and only consider CSIRTs in the educational or research areas. 5 years or so ago, when those areas more or less **were** the Internet in Europe, that may have been a viable approach – but clearly not anymore– it has become impossible to single out a “research island” inside European networking. Therefore this limitation will not be pursued [10].

[9] Like CERT/CC, CIAC, AUSCERT etcetera.

[10] Neither was it by TERENA, not even in the recent past: note e.g. that the late EuroCERT’s services were not limited either to the primary TERENA constituency that had set up EuroCERT.

There is a more practical way to limit the scope, and that is to state what kind of CSIRTs we are interested in for the sake of this report. That list is surprisingly short:

- ISP teams (both commercial and non-commercial);
- Government related teams (including military and law enforcement);
- Vendor teams (with regards to the security of their products, not their internal security);
- Teams for major international institutions or companies including vendors (served by several ISPs);
- Major commercial service providers that offer incident response and strongly related services (providing an "outsourced" CSIRT for the customers).

Agreed, this is a somewhat arbitrary list, but utterly practical. It leaves out the big numbers of (potential) CSIRTs because it hides all those behind ISPs – leaving the building of a “web of trust” for the ISP customers to the ISP itself. As it should be: an ISP delivers a service, so must take care of the essential security aspects of that service, which must include the ability to “handle complaints” (i.e. handle incident reports).

To conclude: the CSIRT scope of this report is limited to (potential) CSIRTs within TERENA members (mainly research ISPs), commercial ISPs, major companies and governmental institutions, plus vendor-product teams and major commercial CSIRTs – all inside “bigger” Europe. As remarked in the preceding chapter we shall concentrate on organisations in phases II or higher – those that realize that they have to actively deal with security incidents – canvassing organisations that are clueless in this respect is outside the scope of this report.

6 Early 2000 considerations (iv) -- Trusted Introducer

What we originally set out to do was to describe a process of introduction and accreditation of new CSIRTs - in order to bring them into "the web of trust" – and to set criteria to foster the **objectivity** and authenticity of this process. With the work done until now, we could revise that aim to include the CSIRT scope limitation and make it more explicit in mentioning that we are interested in the transfer from phase II to IIIa and eventually IIIb, plus the maintenance of that phase. This would be the work for what we already named a *trusted introducer*.

However, for a *trusted introducer* to **verifiably** work, the subjective "belonging to the web-of-trust" parameter used to distinguish between CSIRT phases IIIa and IIIb is no good. Neither are the differences between phases I, II and III very useful in this regard, because though they are fairly objective parameters, they are hard to *show* in an **objective** way. The only way a *trusted introducer* is going to work is taking an essentially empirical approach: collect data, apply templates, establish the authenticity of information and maintain it. That's *TI* in a nutshell:

*We shall refer to the **trusted introducer** as **TI** in this report from now on. We shall apply the term in a generalized sense, where TI means both the process itself and/or the party/parties implementing the process.*

So, when you look at it from the perspective of already established CSIRTs, *TI* must ensure the replacement of trust by expectations – expectations that are based on objective statements that are verifiable:

*The aim of this report is to describe **TI** : an objective process meant to be applied to teams within the above defined scope, that will enable teams new to the CSIRT community to move to a **level** where other teams will find it relatively easy to share information with them and work with them on incidents (in other words: to **trust** them) – and that will enable teams (also the already established ones) to **stay on that level**. To ensure the process's objectivity **TI** will be fully based on objective statements that can be verified – these statements will be worked out in detail, in the form of criteria.*

To avoid TI becoming an abstract framework we now go on to move that the Trusted Introducer be set up as a real life entity – at least inside Europe starting in 2000.

What needs to be done next to substantiate TI is a process description and establishment of objective criteria. Both will be treated briefly now::

5.1 TI process

The CSIRT phases recognized in preceding chapters **are** a convenient way to categorize whether a CSIRT is still in its infancy or whether it has already matured and become accepted. So if the phase scheme is subjective for *TI* purposes, as we argued above, we should replace it by an objective scheme which **does** suit *TI* purposes. Such a scheme can only be based on the information about a CSIRT availavable to TI, and the authenticity of that information. We propose the following scheme, where CSIRTs belong to one of three levels:

- **Level 0:** Information about the CSIRT is available [11]which indicates that the team is within the scope of *TI*.

- **Level 1:** The CSIRT is in the pre-level-2 phase of *TI*, with only 2 possible outcomes: upgrade to Level 2, or fallback to Level 0 after a limited period of time.

- **Level 2:** A well-defined set of information about the CSIRT is available verifiably obtained from individuals *verifiably* [12] representing the team, thus ensuring[13] *authenticity*. The team participates in *TI*, meaning that the CSIRT also complies with a well-defined set of objective criteria (one of which is establishing the information set).

[11] Information available through existing CSIRTs, TI network, RIPE & ARIN databases etcetera.

[12] *Verifiably* means that at least the personal ID is checked and the individual can prove his/her right to represent the team and/or its parent organization.

[13] „ensuring“ in this report should always be read statistically, i.e. if something is ensured, there is a high probability – definiton of „high“ deducible from the context - that it is so: in matters of security there is no such thing as absolute certainty (if there ever is).

The TI process and task then essentially becomes a very simple one:

- maintain a list of Level 0 CSIRTs and an associated public repository;
- advocate the TI process with the intention of inviting teams to go to Level 2;
- assist teams in reaching Level 2 status;
- maintain the list of Level 2 CSIRTs and the associated repositories [14] ;
- assist teams in maintaining their Level 2 status.

5.2 Objective CSIRT Criteria (for Level 2 teams)

When talking about criteria for CSIRTs it needs stating at this stage that these criteria will be based on CSIRT statements (passive or active). And these CSIRT statements
have three properties that we want to distinguish between here:

- Authenticity;
- Actuality;
- Correctness.

Authenticity means that we can be sure the statements came from the CSIRT and/or its parent organisation. We include *integrity* of information (the unmodified transfer from one party to another) along that path of course: if the integrity of information is not assured then its authenticity is meaningless.

Actuality means that the statements reflect the current state of affairs, and not one of a past long forgotten. Actuality can only be achieved when statements are maintained: *maintenance* and *actuality* are two sides of the same coin.

Correctness means that the statements are more than authentic and actual: they are met by reality. This can only be checked by – essentially – performance or quality *measurements* of a CSIRTs work. In certification processes of CSIRTs correctness of information would play a major role.

[14] Apart from the obvious public repository it is advisable to also have a repository with access restricted to Level 2 teams, featuring an extended set of information useful to the Level 2 teams.

*For **TI** purposes we shall concentrate on the **authenticity** and **actuality** properties of CSIRT statements alone: to also check **correctness** would be to attempt some sort of certification which is way beyond scope [15]. We are convinced that certification of CSIRTs **will** take place in some shape in future, but for the coming few years it is clearly a bridge too far: the CSIRT scene is still far too young to bear rigid schemes of this kind.*

However, clearly a Trusted Introducer that does its work well will be regarded as "sort of a certifier" anyway. Let's give it a name: *accreditation* is the word for what TI intends to do – not certification.

What's the criteria then? We propose them to be very simple initially, and essentially as follows:

CSIRTs have to demonstrably comply with the following criteria to reach and maintain Level 2 TI status:

- Fill out well defined templates (see appendix B) with data on CSIRT and its services;
- Define information handling policy;
- Agree to publication of supplied information (only partially in public repository);
- Regularly maintain supplied information;
- Cooperate with TI in matters above;
- *Recommendation only :* Adhere to [RFC-2350];
- *Recommendation only :* Visit FIRST and TF-CSIRT [16] events.

A more detailed list of criteria is offered below.

[15] Numerous discussions within the community of CSIRTs have shown to the authors, that certification is not well received by the majority of teams. It will take more time to convince especially teams not coming from a business environment, where service level agreements are fundamental to any service offer, to realize the business need. On the other hand, especially in the research and educational environment, there seems to be no need from the constituency, to negotiate service level agreements with CSIRTs – our comment would be: maybe not yet, but the need will no doubt arise there as well.

[16] TF-CSIRT is a TERENA task force by and for European CSIRTs, meeting a few times a year and entertaining small scale projects. See http://www.terena.nl/task-forces/tf-csirt .

7 Trusted Introducer Today

To make a long story short: based on the above analysis and recommendations TERENA and its members decided in the Spring of 2000 to start a corresponding TI service on September 1st 2000. The contract was won by Stelvio of Amersfoort, The Netherlands.

To be able to review the operation of TI – additional to an annual contract renewal procedure – a board of representatives of Level 2 teams [17] convened by TERENA was established. This *TI review board* reviews the operation of TI and addresses all special issues that result from its operation. The board performs the following tasks:

- Evaluate four-monthly reports by TI;
- Review the overall performance of TI and handle all complaints about its function;
- Sign the PGP keys of TI to foster the authenticity of these keys;
- Set and change the operational framework for TI;
- Decide about special issues with regards to Level 1 and 2 status, like making exceptions to the set TI rules for Level changes (1 to 2, or 2 to 0), deciding on a site visit to clear issues not clearable otherwise, etcetera.

The board has the right to review the archive maintained by TI at any time to clarify complaints about TI directed to the board and to be able to review overall performance.

The first thing that had to be made more explicit to get TI up and running was the set of CSIRT Level 2 criteria, and the TI process itself. The result is detailed in the TI public repository: http://www.ti.terena.nl/ . We will shortly go into both subjects now:

6.1 CSIRT Level 2 Criteria

A Level 2 CSIRT must/should meet the below criteria. The MUSTS are criteria which have to be met to successfully pass the process and to acquire/maintain the Level 2 status, the SHOULDS are strong recommendations (MUST and SHOULD are defined according to IETF standards, see Appendix A).

[17] Initially consisting of well known and trusted European CSIRT and NREN individuals, to solve the bootstrap issue: when TI started there were no Level 2 teams registered yet, hence the TI Review Board could not consist of Level 2 team representatives.

1. Teams MUST be described by qualitative and a minimum level of quantitative values (basic set of information and services offered) as per Appendix B.

   Teams MUST cooperate with the publication of the delivered data on the TI **restricted-access** website. Access is restricted to Level 2 CSIRTs, the TI and the TI review board.

2. Teams MUST cooperate with the publication of the essentials of their contact information – meaning the items marked 🕮 in the completed Appendix B – on the TI **public** website (http://www.ti.terena.nl/).

3. Teams SHOULD present their service to the outside world as per [RFC 2350], including a specification of quantitative values (advanced set of information).[18]

   Teams MUST adhere to their description as per [RFC 2350] including all service level statements therein – if existent.

4. Teams MUST actively support the TI requirement to keep the information they provided to TI up-to-date, that is to ensure the ***actuality*** of the sent-in templates etc. This criteria of ***actuality*** maintenance also applies to SHOULD criteria.[19]

5. Teams MUST handle all sensitive or private information sent to them – including all incident related information - in a secure and protective way (subject to local law), internally but also when sending it out again. Teams MUST describe their modus operandi in that respect, by filling out the “Information Handling Policy” field of Appendix B. Teams are advised to establish a secure communications scheme based on PGP and / or S/MIME in order to help meet this goal.

6. Teams MUST support question-and-answer sessions (per e-mail in principle) with TI to clear problems or questions arising with regards to the provided information, its ***authenticity*** or its ***actuality***.

[18] Teams are advised to model their service descriptions as indicated in Appendix B, before attempting to fill in [RFC 2350]. Any quality assurance parameters set when applying Appendix B should be reflected as service level statements inside the [RFC 2350] description.

[19] If the CSIRT has chosen to follow those should’s and send in the related information – noblesse oblige: if extra information – in itself praiseworthy – becomes unreliable information, then it will turn against itself and defeat the reliability of even the good information.

7. Teams MUST support (not financially) a site visit if TI concludes that a site visit is necessary. Site visits are last-resort possibilities if question-and-answer sessions fail or when other pressing reasons exist – but a site visit can also be invited.[20] Observations made during the site visit bearing a relation to the criteria described here, will be journalled by TI objectively.

8. Teams SHOULD attend FIRST conferences, TF-CSIRT meetings and other TI supported CSIRT meetings.

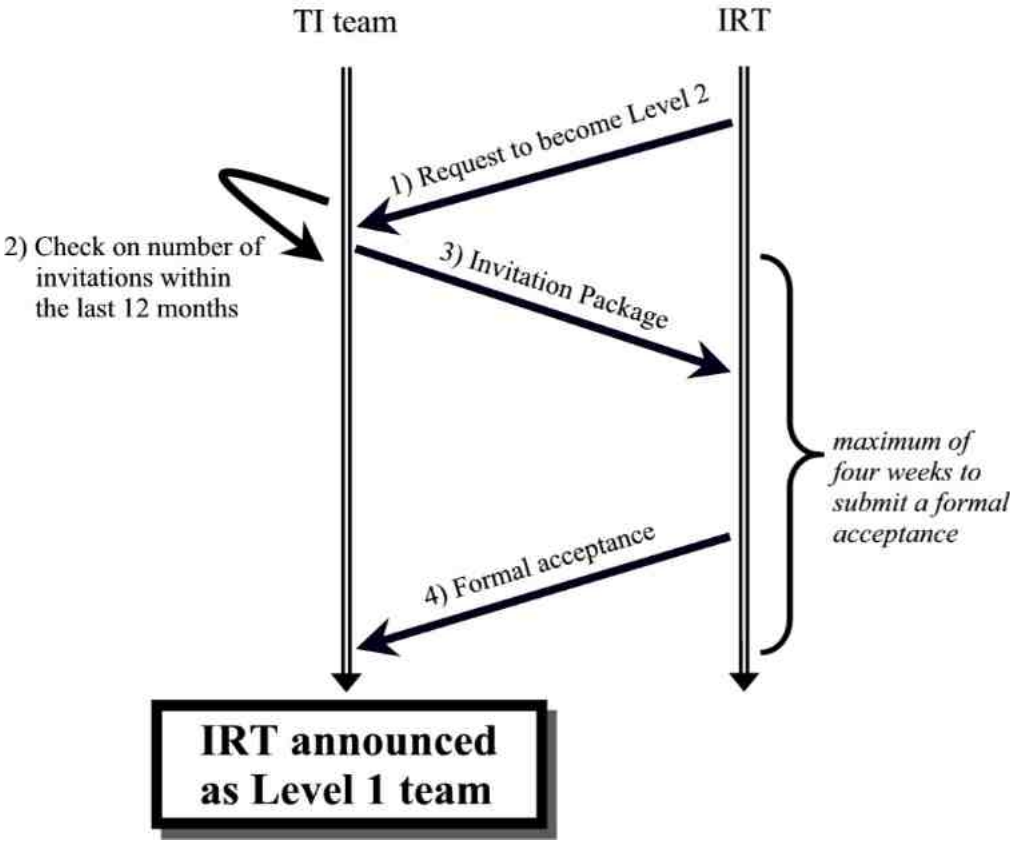
[20] At a site visit TI will naturally limit its scope to the criteria described here – no extra criteria will be set, for that would inevitably lead towards an attempt at certification, which is out of scope.

6.2 TI Process

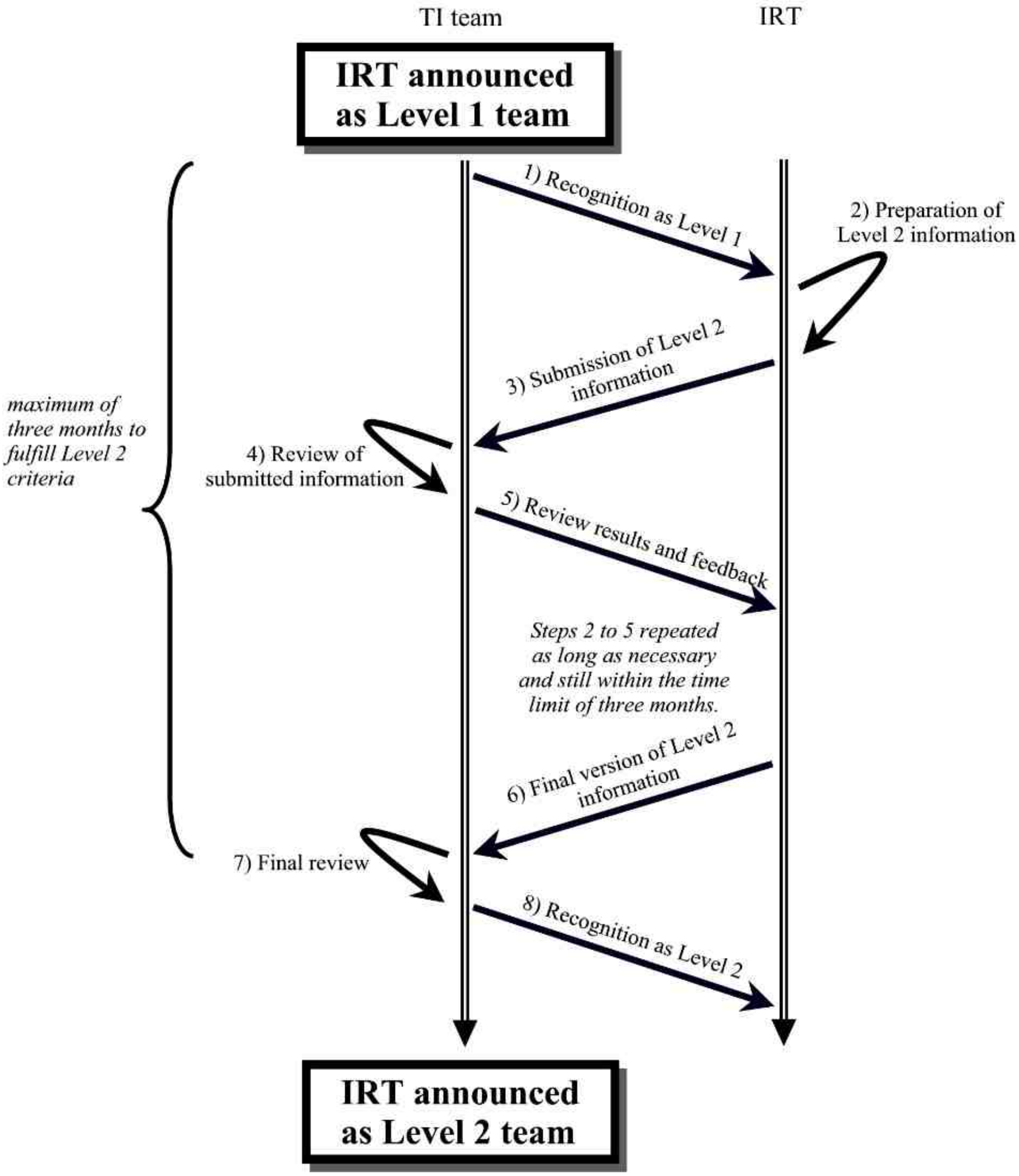
The main task of TI is to advocate, operate and guard the accreditation process that brings CSIRTs from Level 0 ("known" team) to Level 2 (accreditation finished, maintenance cycle started).

The maintenance of the list of all known or Level 0 CSIRTs in the public TI repository is where it all starts. Any CSIRT or CSIRT function (inside Europe) that TI knows of or that is reported to TI will go into that repository. Templates are available to help ease of maintenance. Though essentially a best-effort service, there is active maintenance: CSIRTs that do not react to update questions get tagged "no information since …".

Next thing is that CSIRTs decide they want to go for Level 2 status, by their own request or after an invitation by TI. The process then simply is that TI sends the CSIRT an official Invitation Package with all relevant information. The package includes a form the CSIRT has to sign and send back within four weeks. If they do, the teams goes to Level 1 status and is announced as such in the TI repository. Graphically:


TI team
IRT
1) Request to become Level 2
2) Check on number of invitations within the last 12 months
3) Invitation Package
maximum of four weeks to submit a formal acceptance
4) Formal acceptance
IRT announced as Level 1 team

Once the team has Level 1 status it has to reach Level 2 status within 3 months – or otherwise fall back to Level 0. The process of going to Level 2 is fully described, the essential thing is to fill out two templates, Appendix B below, plus a template describing (yes/no plus explanation) the CSIRTs compliance with the TI CSIRT criteria. TI reviews the material provided by the CSIRT and gives feedback. Once the templates and the information they provide are thus sanitized by CSIRT and TI, and providing all MUST criteria are met of course, TI officially announces the CSIRT as Level 2 team. Graphically:


TI team
IRT
IRT announced as Level 1 team
1) Recognition as Level 1
2) Preparation of Level 2 information
3) Submission of Level 2 information
maximum of three months to fulfill Level 2 criteria
4) Review of submitted information
5) Review results and feedback
Steps 2 to 5 repeated as long as necessary and still within the time limit of three months.
6) Final version of Level 2 information
7) Final review
8) Recognition as Level 2
IRT announced as Level 2 team

The filled-out Appendices B of the Level 2 CSIRTs are made available in full to all Level 2 teams through a restricted TI repository. In the public TI repository only a small part of that information – mainly constituency and contact data - is made available to the world.

Last part of the process is the maintenance of Level 2 status. At least every four months the Level 2 teams have to acknowledge that the information they provided is still correct and up-to-date – preferably the CSIRTs actively pass-on changes to TI to incorporate into the trusted repositories. If a CSIRT fails to comply to the maintenance cycle, or does not meet all MUST criteria anymore at some stage, the team falls back to Level 0 eventually.

All processes operated by TI are fully described processes, based on measurable, objective criteria. In those unlikely cases where CSIRTs do meet and continue to meet all TI criteria but still fail to function as a CSIRT – for example becoming apparent by serious complaints of fellow CSIRTs – there is also a mechanism that can lead to a Level 0 downgrade. This passes necessarily through the TI Review Board however, since it is essential that TI upholds its objective character.

Clearly TI and TI Review Board will go to some lengths to avoid downgrades to Level 0 – the success of the TI framework is dependent on a well-filled, reliable TI repository. However, “reliable” always takes precedence over “well-filled” – so if a team demonstrably fails to comply to the framework, it will be confronted with this.

8 Management Summary

The Trusted Introducer (TI) mission statement:
The Trusted Introducer must foster trust and cooperation between *CSIRTs in Europe, both new and experienced. The vehicle used to achieve this is to invite CSIRTs to present themselves and describe their service according to an established baseline – thus enabling objectivity, which is regarded as the pre-requisite of trust.*

The TI organisational setup:

- European NREN society TERENA enables TI for **all** (no NREN focus!) European CSIRTs and channels funding;
- TI is subcontracted to Stelvio of Amersfoort, The Netherlands;
- TI Review Board with representatives of CSIRTs reviews TI work and deals with special cases;
- All details: http://www.ti.terena.nl/ .

The TI process:

- TI registers “known” European CSIRT teams as Level 0;
- Teams that decide to join the TI effort to foster European inter-CSIRT cooperation get invited by the TI to become Level 1;
- The Level 1 team then has 3 months to work together with the TI to present their service according to the TI baseline and meet the Level 2 criteria;
- If they succeed, the team is recognized by the TI as Level 2 and their baseline presentation is published in the TI repositories (only partially in the public repository);
- Level 2 teams maintain their status by regularly complying with their baseline presentation – or adapting it when due;
- Any non-compliance to the above process results in a fallback to Level 0.

TI criteria for Level 2 CSIRTs include:

- Fill out well defined templates (see appendix B) with data on CSIRT and its services;
- Define information handling policy;
- Agree to publication of supplied information (only partially in public repository);
- Regularly maintain supplied information;
- Cooperate with TI in matters above;
- *Recommendation only :* Adhere to [RFC-2350];
- *Recommendation only :* Visit FIRST and TF-CSIRT events.

TI does *not* offer you:

- FIRST membership:
  - FIRST: only worldwide CSIRT forum;
  - FIRST offers nothing like TI yet;
  - TI Level 2 teams are well prepared for FIRST membership;
- A free ride:
  - Initial fee to go to Level 2 (mainly high level consultancy) under Euro 1000;
  - Level 2 maintenance costs Euro 600 per year.

TI *does* offer you:

- Public and maintained repository of all “known” or “Level 0” European CSIRTs with contact info;
- Formalized and published accreditation process for CSIRTs: those that pass it are “Level 2” CSIRTs --- maintenance is ensured;
- Maintained trusted repository for Level 2 CSIRTs only, offering extended information on all members.

9 References

[RFC 2119]
Key words for use in RFCs to Indicate Requirement Levels / Scott Bradner. - Request For Comments 2119.

[RFC 2350]
Expectations for Computer Security Incident Response / Nevil Brownlee ; Erik Guttman. - Request For Comments 2350.

[West-Brown et al. 1998]
Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J. West-Brown ; Don Stikvoort ; Klaus-Peter Kossakowski. - CMU/SEI-98-HB-001. - Pittsburgh, PA: Carnegie Mellon University, 1998.

[Kossakowski et al. 1999]
Responding to Intrusions / Klaus-Peter Kossakowski ; Julia Allen ; et al. - Security Improvement Module CMU/SEI-SIM-006. - Pittsburgh, PA: Carnegie Mellon University, 1999.

Appendix A: Standard definitions taken from the IETF approach [RFC2119]

MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

Appendix B:
Basic Set of Information

The basic set of information consists of three parts, one mandatory and one optional part are related to the team itself, the other mandatory part is related to the task of the TI. The whole set of information will be published on the restricted TI web site.

The sub-set of information that will be published on the public TI web site is marked below with the symbol "🕮".

Mandatory Fields describing the Team

Team Name 🕮

Official team name.
Short team name (Acronym).
Host organization (if the team is decentralised, list all host organizations).
Country the team is located in (if multiple offices exist, list all countries).
Date of establishment.

Constituency 🕮

Type of constituency (vendor customer base, internal to host organization, ISP customer base, ...).
Description of constituency.
Internet domain, AS numbers and/or IP address information describing the constituency.
All countries in which constituency members are located in.

Team Contact Information 🕮

Regular telephone number (country code, telephone number, timezone).
Emergency telephone number (country code, telephone number, timezone).
E-mail address.
Facsimile number (country code, telefax number).
Other telecommunication facilities.
Postal address.

Business Hours

Description of business hours. 🕮

Procedures for contacting the teams outside business hours.

Team Representative

Name of person representing the team.
Contact information.

References

Track record of working relationships with other teams.

Services

[The following lists of services are only meant as examples.]
Specify available reactive services, using the following list (or adding to it):

- vulnerability analysis;
- critter analysis;
- forensic analysis;
- incident response;
- incident response support;
- incident response coordination;
- vulnerability response coordination.

Specify available proactive services, using the following list (or adding to it):

- announcements (intrusion and vulnerability advisories);
- technology and trend watch;
- security audit and neighbourhood watch;
- configuration/maintenance of security tools;
- development of security tools;
- provision of intrusion detection services.

Specify security quality management services, using the following list (or adding to it):

- risk analysis;
- business continuity planning;
- security consulting;
- awareness building and training;
- product evaluation.

Information handling policy

How is incoming information “tagged” or “classified”?
How is information handled, especially with regards to exclusivity?
What considerations are adopted for the disclosure of information (“when what?”), especially incident related information passed on to other teams or to sites?
Are there legal considerations to take into account with regards to the information handling?

Cryptography

Policy on use of cryptography to shield confidentiality and integrity in archives and/or in datacommunication, especially e-mail.
This policy must include possible legal boundary conditions as key escrow or enforceability of decryption in case of lawsuits.
If encrypted e-mail is possible, then at least provide:

- PGP[21] key of Team Representative;
- PGP "team" and / or "master" keys if applicable; 📖
- Provision of X.509 certificates is optional. 📖

FIRST Membership 📖

Membership status (No member / FIRST Member/ FIRST Liaison).
In case of Member or Liaison: date of member/liaisonship approval.

Optional Fields describing the Team

Team Members

Names, contact information and PGP keys / X.509 certificates of other team members.

Technical Expertise

Operating Systems.
System Platforms.
Networks.

Contact Information for Constituency / Host Organization

Contact information for person/organization representing the constituency.
Contact information for person representing the host organization.

PGP Key Revocation Certificates

Key Revocation Certificates for previously distributed PGP keys.

Information Server

Public WWW server. 📖
Other WWW server.
Mailing lists.
(Anon)FTP server.
NetNews.

[21] For all practical considerations PGP (Pretty Good Privacy) is the established standard for providing confidential and authentic communication within the CSIRT community.