Minutes of the first and second TI Review Meeting
1st September 2015, 3pm CEST via WebEx
14th September 2015, 3pm CEST via WebEx

In Attendance 1st September 2015: Vladimir Bobor (chair), Serge Droz, Lionel Ferette, Nicole Harris, Sigita Jurkynaite, Andrea Kropacova.

In Attendance 14th September 2015: Vladimir Bobor (chair), Lionel Ferette, Nicole Harris, Przemek Jaroszewski, Sigita Jurkynaite, Andrea Kropacova.
Apologies 14th September 2015: Serge Droz.

1. Overview

NH gave an overview of the terms of the WG and the approach proposed, including the two-phase approach to the review that can be found in the terms of reference.

2. Service Review

VB gave an overview of the services / requirements from the call for proposals and what was requested during the last tender. Participants agreed to review the work areas and discuss whether they are still seen as requirements for a future service. The discussion is represented in the table below.

Requirement	Status	Discussion
Technical Requirements		
A1. Provision and maintenance of an electronic registry providing contact information for listed, accredited and certified CSIRTs.	Green	Essential and fundamental part of the service offering.
A2. Provision of a Certificate Authority and issuing X.509 certificates to official representatives of accredited CSIRTs and TI Associates.	Amber	It is essential for teams to be able to obtain certificates, but it is a requirement of the TI service operator itself? Could TCS be used or other options?
A3. Signing PGP keys of CSIRTs and their representatives.	Green	Essential part of the service offering.
Membership Management		
A4. Listing and accreditation of CSIRTs according to the criteria agreed by the TI community.	Amber	Essential part of the service offering. However it was felt that improvements could be made to the way in which teams are accepted and approved for accreditation – for example asking for community approval of the accreditation process in a manner similar to requirements for initial list. Teams expressed concerns that there was not enough awareness or

		vetting in the community of accreditation standing.
A5. Re-verification of information of accredited CSIRTs at least once every four months, and taking appropriate action in the event of failure by a CSIRT to re-verify or to pay its service fees.	Green	Essential part of the service offering.
A6. Re-verification of Listed CSIRTs on an annual basis.	Amber	Essential part of the service offering. Concern that this is not being followed by TI team.
A7. Handling the admission and re-admission of TI Associates according to the criteria agreed by the TF-CSIRT Steering Committee.	Green	Essential part of the service offering.
A8. Assessing CSIRTs for certification status (including an on-site workshop) according to the criteria agreed by the TI community. This includes re-verifying information every four months, and re-certification every three years.	Amber	Could we use the community more rather than just relying on the TI team to do this? It would be more like the FIRST model and would raise certain issues but it could change the process. There would be the need for a pool of vetted certifiers, very much like there is a pool of TRANSITS teachers. + This strengthens the community - More difficult to maintain consistency and levels.
Event Management		
A9. Provision of a system to all event bookings made for TF-CSIRT meetings and to record team attendance at meetings. The administrative interface should be accessible by the TF-CSIRT Secretary.	Amber	Noted that this is not currently part of the service offering but that TI are looking to provide an IdP to allow people to more effectively use existing GÉANT systems. Change this to a "tracking system for teams attending" requirement rather than expressed as event management. Is this overkill? Could this not just been done by filling in a spreadsheet or counting the pieces of paper? This should tie in to the benefits for the teams – i.e. an airmiles type approach.
A10. Organising closed sessions at TF-CSIRT meetings and / or other appropriate locations according to the TF-CSIRT Terms of Reference.	Amber	Should the closed meeting be organised by the TI team? Should the whole meeting be the responsibility of one organisation – e.g. move the organisation to the same people as the open meeting or vice versa. The division is currently not very effective. The community should always drive the agenda for meetings. The reason that this works currently is that the TI Team is very

		much part of the community – general outsourcing would not work.
A11. Logistical support for elections and votes at TF-CSIRT meetings.	Green	Essential part of the service offering.
Reporting		
A12. Provision of regular reports to the TF-CSIRT Steering Committee on service uptake and use. This reporting should also include proposals for new ideas to improve and enhance the TI service over the contractual period.	Green	Essential part of the service offering.
A13. Attendance at TF-CSIRT Steering Committee meetings.	Green	Essential part of the service offering.
Support		
A14. Management of a helpdesk for existing and potential TI members.	Green	Essential part of the service offering.
A15. Provision and maintenance of public and restricted TI websites where service and contact information is published.	Green	Essential part of the service offering.
A16. Provision and maintenance of mailing lists and other tools to support communication with and between service users and the formation of working groups under the TI umbrella.	Amber	Mailing list(s) are an essential part of the service. Alerting system – this is not feasible anymore in today's environment and perhaps not a future requirement, as telephony and internet have pretty much merged. IRC server the need for a certificate makes this service cumbersome to use, and usage is low.
Outreach		
A17. Engagement in outreach activities to bring in new members to TI.	Amber	Essential part and one of the unique elements of the work that Presecure currently do. The service needs to have this standing in the community. Would be useful to have someone on the steering committee with a remit to oversee this. Changing wording to support this rather than specifically be active. Should this just be part of member management?

These additional areas were included in the Presecure Trusted Introducer response to the last tender.

Requirement	Status	Discussion
Additional Services Offered		
A18. Printed Status Certificates	Green	Useful service – perhaps link to proposal from Zuzana for logos.
A19. Handling IRT Objects	Amber	Seen as valuable – completing information held by RIPE is not an easy task and members benefited from the automation. However more could be done to better understand the purpose of the information and how it is used – in general terms the work relationship with RIPE could be expanded.
A20. Incident / Vulnerability Coordination	Amber	Currently described as best efforts – does this need to be a definite service? Not a specific requirement of the tender.
A21. Recognition of the TF-CSIRT Liaison Members	Green	Has become increasingly important and should be seen as part of the core offering.
A22. Supporting the Invoicing Process	Grey	This is not a service in itself but describes how other services are delivered.
A23. Staffing	Grey	This is not a service in itself but describes how other services are delivered.
A24. Business Hours and Service Levels.	Grey	This is not a service in itself but describes how other services are delivered.
A25. Service related Points of Contact.	Grey	This is not a service in itself but describes how other services are delivered.
A26. Networking and Email Infrastructure.	Grey	This is not a service in itself but describes how other services are delivered.
A27. PKI Infrastructure	Grey	This is not a service in itself but describes how other services are delivered.
A28. Server and Services	Grey	This is not a service in itself but describes how other services are delivered.

3. Potential New Services

3.1 Information Sharing Infrastructure.

There has been discussion that to operates infrastructure to help facilitate information sharing. This could be AS numbers a CERT is responsible for, or domain names.
If it is felt that there is a need for this, TI could provide this service. I feel it's imperative though to collaborate with existing provides, in particular RIPE, which already collects abuse addresses for ASNs and IPs. Suggestions for work in this area include:

- Building on relationship with RIPE and define some specific things to work on together.
- Regular maturity tests.
- Current database is not very usable – an API would be a very valuable service.

- Perhaps look at some mock tests for gathering this information by the TI team to see if appropriate scripts are working to gather information. Aaron's tool?

3.2 Training Exercises / Skill Level of Teams

What is the relationship between TI and the teams in terms of ensuring that the teams are "well skilled". The accreditation and certification process assesses this to some extent, and the recent reaction / maturity testing also supports this process. TI could be asked to run more training exercises to support the process.

In terms of exercises, it was felt that this might be more applicable for certain types of teams (e.g. NRENS, emerging teams). Other teams already engage in many different exercises every year and it would not be a good use of resource. It would be interesting to see if we could get some statistics on teams participating in training at ENISA / TRANSITS etc.

Andrea offered to prepare some information on the full range of exercises that the Czech teams have been involved in to show the impact of this training. It would also be interesting to look at the relationship between TRANSITS and TI and how we record information about attendance at TRANSITS courses.

4. Agenda Proposed for the Second TI Review Meeting

At the next meeting of the TI Review group it was agreed that participants should discuss:

- The additional services offered in the Presecure tender (see table below). Some of these fall more in to the category of contract points rather than requirements / service offering.
- List of requirements not currently offered by the service (e.g. maturity testing, fire drills etc).

It was also agreed that areas flagged as amber should be discussed in more detail with the community, either at the upcoming TF-CSIRT meeting or via email channels.

5. Agenda Proposed for the Third TI Review Meeting

At the next meeting of the TI Review group it was agreed that participants should discuss:

- Firming up issues shown in Amber and new service ideas into fairly well defined proposals that can be considered by the community.
- Looking in more detail at the current accreditation / certification processes to see if more detailed changes should be suggested in these areas.
- Process for consulting with the community on ideas –email, survey, presentation etc.

6. Timetable of meetings

The timetable for meetings of the TI Review Group will be:

- 1st September 2015 at 3pm CEST (via WebEx).

- 14th September 2015 at 3pm CEST (via WebEx).
- 25th September 2015 following the TF-CSIRT meeting (face-to-face).