**Minutes of the Third TI Review Meeting**
**25th September 2015: Tallinn, Estonia.**

**In Attendance:** Vladimir Bobor (chair), Lionel Ferette, Nicole Harris, Przemek Jaroszewski, Sigita Jurkynaite, Andrea Kropacova, Dave Monnier, Wilfried Woeber.

**Apologies**: Serge Droz (on vacation).

## 1. Welcome and Agenda Review

Vladimir Bobor welcomed members of the TI Review Committee to the meeting. Members agreed the agenda proposed at the second TI Review Meeting.

## 2. Amber Issues

Members reviewed the issues identified as "amber" in previous meetings and agreed next steps proposals for each area. These are shown in the table below.

| Requirement | Discussion on next steps |
|---|---|
| A2. Provision of a Certificate Authority and issuing X.509 certificates to official representatives of accredited CSIRTs and TI Associates. | It is not clear that we have a requirement for a CA.<br><br>The more services that are bundled in centrally, the reliance we have and the more difficult in moving the service from Presecure.<br><br>Reframe the requirement to say that we require a secure website, and leave it open to how this is provided. The offering should be complete though – e.g. no requirement for teams to buy tokens etc. |
| A4. Listing and accreditation of CSIRTs according to the criteria agreed by the TI community. | If there is not complete transparency in the process than problems come into the system. It is also important that this is retrospective, particularly when processes are changed.<br><br>Make it clear that when there have been teams that did not go through the full process then we need to highlight that these have been grandfathered.<br><br>Ask TF-CSIRT SC to carry out a document review of current accreditation documentation.<br><br>If these actions are achieved within this cycle then this area can move back to green. |
| A6. Re-verification of Listed CSIRTs on an annual basis. | Listing should expire at some point – perhaps introduce a three-year cycle and remove listing if it is not updated.<br><br>Clarify the expectation of listing. What level of quality do we want from the listing? |

| | |
|---|---|
| | Need to take this back to the community. Must be updated or confirmed within a set period of time.<br><br>Work on the accreditation "package" to see how we are marketing it to the teams and review whether enough is offered in accreditation. Think about added value of accreditation and the gamification ideas around response testing.<br><br>Get mature CERTS to help with encouraging CERTS within their areas.<br><br>Consider giving more benefits to those offering commercial services. |
| 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. | Question about whether we can use the community more for certification. Benefits of scalability and more knowledge base but problems with how we ensure the quality.<br><br>Would require training, small focused group.<br><br>Take the proposal back to the community for consultation. |
| 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. | Requirement needs rewording for the future. |
| A10. Organising closed sessions at TF-CSIRT meetings and / or other appropriate locations according to the TF-CSIRT Terms of Reference. | Reword to be logistical support.<br><br>Review approaches to admitting people to the closed meeting. |
| 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. | No requirement for the alerting system.<br><br>Mailing list(s) are an essential part of the service.<br><br>IRC server the need for a certificate makes this service cumbersome to use, and usage is low, not required. |
| A17. Engagement in outreach activities to bring in new members to TI. | Remove. |
| A19. Handling IRT Objects. | No longer required. |
| A20. Incident / Vulnerability Coordination. | Should only be offered on a best efforts basis but should not be offered as a contractual requirement. |

**3. New Features**

Members considered new feature requirements collected to date.

| Proposal | Next Steps |
|---|---|
| API for database | Strong support for making this a requirement for future tenders. |
| Training Exercises | This should not be looked at in the context of TI but in the wider strategy and approach of TF-CSIRT. |
| Regular Maturity Testing | Subject to the success of the approach over the next couple of test periods, introduce this as a requirement for future tenders. |
| Extended information set for teams | Would need more information on requirements from the community. |

**4. Finalised Proposals**

The following areas represent the proposals to the community to be introduced in response to the TI review process. The proposals fall into three categories: changes to tender requirements, changes to address in the current service period, recommendations that fall outside of the TI review process.

**4.1 Changes to tender requirements**

CA and X.509 Certificates

4.1.1: The tender should not specifically ask for a CA but instead detail the need for a secure website with managed restricted areas and appropriate credentials for team members. This should be a complete solution and not require teams to purchase additional products (e.g. certificates, hardware tokens etc.). This should include requirements for credentials that can interoperate with the SAML event management services offered by GÉANT.

Certification

4.1.2: Introduce a change to the certification process so that certifications are carried out by a small group of experts from the community (which could include TI staff) similar to the TRANSITS tutors model instead of only managed by TI staff.

Communication Tools / Processes

4.1.3: Alerting services and IRC servers and not required by the community and should not be included in future service offerings.

4.1.4: Incident / Vulnerability coordination should not be a requirement of the tender but could be offered on a best efforts basis.

4.1.5: IRT object process is no longer required as RIPE does not make use of this and is changing its data gathering processes.

Database API

4.1.6: Introduce a requirement in future tenders for an API to the TI database.

Maturity Testing

4.1.7: subject to further testing, introduce a requirement in future tenders for regular maturity testing.

**4.2 Changes to address in current service period**

Listing / Accreditation

4.2.1: Ask the TI team to complete a short internal audit to ensure that all appropriate alerts around listing / accreditation are being delivered.

4.2.2: Ask the TI team to flag listed teams that received listing status before the requirement for support was introduced and accredited teams that may have received accreditation status without explicit support.

4.2.3: Introduce a new process for listing whereby teams that do not update or actively confirm data is up-to-date within a three-year period automatically become unlisted.

Meeting Support

4.2.4: Ask the TF-CSIRT SC and TI team to review the process for managing entry to the closed meeting and whether more effective approaches could be used.

4.2.5: Move management of the agenda for both closed and open meetings to the GÉANT secretariat to allow for more consistency in meeting management process and work with presenters to more accurately reflect TLP status. This could include moving out of closed session at different times when appropriate.

**4.3 Recommendations that fall outside of review process**

Accreditation Documentation and Support

4.3.1: Ask the TF-CSIRT SC to manage a review of the accreditation process documentation and proposed appropriate updates.

4.3.2: Work on the accreditation "package" to see how we are marketing it to the teams and review whether enough is offered in accreditation and provide more materials to help teams explain the value of accreditation to management.

Listing Requirements

4.3.3: Consider using mature CERTS to help encourage other CERTS within their region to keep listing information up to date.

Service Strategy

4.3.4: Ask the TF-CSIRT to work on a strategy document for TF-CSIRT / TI and a mission statement for the service offering. This should include clarity on the goals of each of the current processes (listing, accreditation, certification). This will be further informed by phase 2 of the review process and should include the full current and future portfolio for TF-CSIRT (e.g. TRANSITS, training exercises etc.).

### 4.4 Communicating Review to Community

Phase 1 of the TI review process is now at a point where the community should be consulted on the proposals to date. Nicole Harris will prepare a communication for the TF-CSIRT mailing list including the reports from the review team and an easy to digest summary of the recommendations in shorter format.

ACTION: TIR150925-01 Nicole Harris to prepare materials for community consultation of TI review proposals and send to the working group for approval.

### 4.5 Next Meetings

Members agreed that it would be appropriate to set up two further meetings following the community consultation – one to review the consultation results and the second to finalise the findings for Phase 1 of the review.

ACTION: TIR150925-02 Nicole Harris to send a Foodle poll for meeting dates in November for discussion after the community consultation has taken place.