Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 08 mars 2016
N° 879/ANSSI/SDE/PSS/CCN

Référence : ANSSI-CC-ANO-P-01/3.0.EN

PROCEDURE

ANOMALY PROCESSING

Application : From date of publication

Circulation : Public

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Version history

Versions	Date	Modifications
1	13/01/2004	Creation
2.0	07/03/2011	Document update
3.0	08/03/2016	Document reorganisation and public circulation

Pursuant to amended decree No. 2002-535 of 18th April 2002, this application note has been submitted to the certification management committee, which gave a favourable opinion.

This application note is available at the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1. Subject of the procedure

This procedure defines the process implemented to resolve all anomalies of all kinds and that relate to the whole certification activity (Common Criteria and First Level Security Certification) and the certification body's quality system.

2. References

- Standard ISO/IEC 17065, chapter 7.13;
- Common Criteria for Information Technology Security Evaluation, current version;
- ANSSI-CSPN-CER-P-01 – First level security certification for information technology products;
- Amended decree No. 2002-535.

3. Definitions

The term *anomaly* is the generic term used to denote *appeals*, *complaints* and *discrepancies*.

- An *appeal* is a request which is sent to the certification body by a sponsor for this body to reconsider a decision which has already been taken in relation to the certification of an evaluated object or the licensing of an ITSEF[1].

  For example:

  - A sponsor may issue an appeal after the certification decision is issued;
  - An evaluation facility may issue an appeal if its licensing is refused.
- A *complaint* is the expression of discontent other than an appeal issued by a person or an organisation to the certification body, in relation to this body's activities, to which a response is expected.

  For example:

  - Identification by a third party that a product marketed with the certification marks does not correspond to the product which was certified;
  - Identification by a third party of false advertising on a product's certification status.
- A *discrepancy* is a non-conformity with the requirements that apply to the certification body (quality system, ISO 17065 standard, CCRA and SOG-IS recognition agreement) identified during an audit (internal or external) or raised spontaneously by certification body personnel.

A *corrective action* is an action which is undertaken to eliminate the cause of an anomaly which is detected or another undesirable situation.

A *preventive action* is an action which is undertaken to eliminate the cause of a potential anomaly or another potential undesirable situation.

An *improvement* is a change advice which does not come from an anomaly. It may or may not lead to an action.

A *dispute* is an appeal which had to be submitted to the Certification Management Committee for a decision to be taken (see chapter 7).

4. Anomaly processing

The Body's anomaly monitoring and actions table (TAC) is created in accordance with ANSSI-CC-ANO-L-01[2]. The first tab in the TAC "Anomalies" deals with the registration and processing of the body's anomalies and is filled in continuously by the quality manager and/or the body's manager.

[1] Information Technology Security Evaluation Facility.

[2] ANSSI-CC-ANO-L-01 "TAC template" list

4.1. Registration

The *anomalies* may be brought to the attention of the certification body in numerous ways: fill in the online form (ANSSI-CC-ANO-F-03[3]), electronic or verbal message, letter, telephone call, press article, audit, etc. The certifier who receives the anomaly alerts the body's manager and the quality manager in writing.

All the members of the certification body may submit an anomaly.

The reception or detection of an anomaly leads to it being registered, if relevant, in the TAC, which specifies:

- The date when the anomaly was received by the certification body's personnel, in the "Anomaly reception date" column;
- Its nature (complaint, appeal or discrepancy) in the "Nature of the Anomaly" column;
- Its origin in the "Source of the Anomaly" column;
- Its description in the "Description of the Anomaly" column;

To make things easier to read, if necessary, an anomaly file may be created in accordance with ANSSI-CC-ANO-F-01[4] and is added to the "Anomalies" sub-file; this link to this file is indicated in the TAC.

If the anomaly comes from the ANSSI-CC-ANO-F-03 form published on the website, the form is then registered and added to the "Anomalies" sub-file; the link to this document is indicated in the TAC.

Once the anomaly is registered, the certification body acknowledges reception of it via paper or electronic mail.

4.2. Cause analysis

The certification body searches for the causes of the anomaly once it is registered.

Once determined, the causes of the anomaly are registered in the "Causes of the Anomaly" column in the TAC.

4.3. Correction

Once the anomaly is registered, the certification body corrects it in due time. These immediate corrections are added to the "Correction of the Anomaly" column in the TAC.

4.4. Information to the issuer

The certification body transmits the conclusions of how a complaint is processed where possible.

The certification body advises the claimant of the conclusions of an appeal process.

[3] ANSSI-CC-ANO-F-03 "External anomaly file" form

[4] ANSSI-CC-ANO-F-01 "Internal anomaly file" form

5. Action processing

The second tab in the TAC "Actions" deals with the registration and processing of the body's actions and is filled in continuously by the quality manager and/or the body's manager.

The analysis of an anomaly's causes may lead to a corrective action as described below.

An improvement, or an observation internal or external to the centre (for example, an internal audit) may lead to a preventive action, as described below.

5.1. Corrective actions

The opportunity to carry out an action to guarantee that the anomalies will not reoccur is determined as shown below:

- If the anomaly's cause analysis shows that it is related to the certification activity, then:
  - Opening of a corrective action
- Otherwise:
  - A response is provided to the person who initiated this anomaly.

5.2. Preventive actions

An improvement may lead to the opening of a preventive action if it has an impact on the quality reference base. Otherwise, processing is carried out inside the certification body.

5.3. TAC update

The TAC is updated according to:

- The nature of the action launched (corrective or preventive) in the "Nature of the Action" column;
- The number of the anomaly, if it is a corrective action, in the "Number of the Anomaly" column;
- The date when the action was opened, in the "Action opening date" column;
- An incremental number is entered for the action;
- A priority is entered;
- The description of the action launched in the "Description of the Action" column; To make things easier to read, if necessary, an action file may be created in accordance with ANSSI-CC-ANO-F-02[5] and is added to the "Actions" sub-file;
- The designation of a processing manager, if necessary;
- The decision on a target date, if necessary;
- The action's status is entered as "open" or "in progress" in the "Action status" column.

5.4. TAC monitoring (STAC)

The STAC is carried out during the regular meeting chaired by the quality manager who decides on the priority and processing time for the action, in agreement with the certification body manager.

The objective of the STAC is to look at all of the anomalies and actions with the certification body and to see their progress. The TAC is updated accordingly and is sent to the certification body.

A set of minutes may also be issued following each of these meetings and then be circulated to the certification body and added to the "STAC" sub-file.

5.5. Results

When the action is implemented, the results are added to the "Action result" column in the TAC. For example, "the procedure was updated". The action's status then changes to "closed".

[5] ANSSI-CC-ANO-F-02 "Corrective-preventive action file" form

6. Verification of the actions' effectiveness

The quality manager is responsible for verifying the effectiveness of the actions which were carried out.

To do so, once they have performed the verification, they enter the following in the TAC:

- The verification method used, for example, the publication of the updated procedure on the website;
- The verification date;
- The verification status changed to "closed".

7. Dispute

If the claimant is not satisfied with the conclusions of the appeal process communicated by the body as indicated in chapter 4.4 and if they request it, the appeal then becomes a 'dispute" under the terms of the reference decree (Article 15).

The certification body then calls on the Certification Management Committee which examines the dispute for conciliation purposes. This mission may be delegated by the committee to one of its members; the parties must then be interviewed.