Swedish Certification Body for IT Security

103 Terms of Reference for the Scheme Advisory Committee

Issue: 14.0, 2020-Feb-04

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Purpose 3

2 Organisation 4
2.1 Membership 4
2.2 Members 4
2.3 Financial terms 4
2.4 Confidentiality 4

3 Operations 5
3.1 Normal operations 5
3.2 Actions when advice is not followed 5

4 Responsibilities 6
4.1 Head of CSEC 6
4.2 Secretary 6
4.3 Members 6

Appendix A Agenda for the SAC-meeting 7

1 Purpose

1 The main purpose of the Scheme Advisory Committee (SAC) is to ensure the impartiality of the operations of the certification body and to enable the participation of all parties significantly concerned in the development of policies and principles regarding the content and operation of the Scheme.

2 In order to fulfil its purpose, the Scheme Advisory Committee shall:

- Monitor changes to the Scheme
- Monitor the Certification Body's handling of identified risks to impartiality
- Monitor the Certification Body's handling of complaints and appeals, and point out any nonconformities to the Scheme regulations.

3 The Scheme Advisory Committee shall provide input on:

- the policies and principles relating to the impartiality of the certification activities,
- any tendency on the part of a certification body to allow commercial or other considerations to prevent the consistent impartial provision of certification activities,
- matters affecting impartiality and confidence in certification, including openness[1].

4 The Scheme Advisory Committee will review the Certification Body's procedures and policies in general, and may propose improvements to the procedures and policies.

5 Through the Scheme Advisory Committee, the members will also have an opportunity to influence the international efforts to improve the Common Criteria standard and methodology within the Common Criteria Recognition Arrangement (CCRA) and the Senior Officials Group Information Systems Security (SOGIS) frameworks, and to be informed about recent developments in the projects and committees of CCRA and SOGIS.

[1] According to ISI/IEC 17065:2012, a certification body needs to provide access to, and disclosure of, appropriate and timely information about its evaluation and certification processes, as well as about the certification status of any product (i.e. granting, maintaining, extending or reducing the scope of, suspending, withdrawing or refusing certification), in order to gain confidence in the integrity and credibility of certification. Openness is a principle of access to, or disclosure of, appropriate information.

2 Organisation

2.1 Membership

6 The composition of the Scheme Advisory Committee shall be such that a balanced mix of different categories of parties with a stake in the Scheme - such as Sponsors, IT Security Evaluation Facilities (ITSEF), government organisations, customers, and others - is preserved. Within each category, a representative selection of individual members shall be made.

- A member of the committee should have good understanding on the implications of information assurance within their organisation and should have substantial knowledge in the area of information security. Membership in the committee is personal. A member who cannot participate at a meeting may on a case-by-case basis propose a replacement representative, whom needs to be approved by the chairman.
- The number of members in the committee should normally be between 10 and 15. Out of these The Head of CSEC is chairman.
- A person submitting a report to the committee need not be member. In such cases the person may participate during the handling of the specific question.
- A member is normally appointed for two years.

7 The exact constitution of The Scheme Advisory Committee is established on a yearly basis after decision by the Head of CSEC.

2.2 Members

8 The Scheme Advisory Committee should have the following representatives:

- The Head of CSEC.
- A secretary, appointed by the Head of CSEC.
- Two members representing Sponsors and certificate users.
- Up to three members representing the ITSEFs active in the Scheme.
- Two IT product developers.
- Members representing government organisations with an interest in IT security evaluation.
- Members representing other parties with an interest in IT security evaluations, such as universities and consultant companies.
- Observers may be invited to the meetings by the chairman.

2.3 Financial terms

- No financial compensation is awarded, neither to the member nor to its organisation.
- A member participates in the committee during regular working hours within the member’s own organisation or during free time.

2.4 Confidentiality

9 All members will have to sign a document where the confidentiality rules the members are required to follow are acknowledged, VB-146 *Erinran och kvittens - CSEC sekretessregler*.

3 Operations

3.1 Normal operations

10 The Scheme Advisory Committee shall meet at least once every year.

11 Between meetings, the Scheme Advisory Committee's advice may be requested by the chair.

12 Meeting invitations shall be distributed to all members at least one month in advance of each scheduled meeting. At least one week prior to a meeting, the agenda and background information shall be distributed to all members.

13 The Scheme Advisory Committee Meetings will be held under the following procedures:

- The Head of CSEC will be the chair of the meeting.
- The meetings will be documented in minutes.
- Swedish will be used as working language.
- Any member owns the right to have comments included in the minutes on request.
- The meetings will be held in Stockholm, unless otherwise agreed

14 The minutes from the meetings shall be distributed to all members of the Scheme Advisory Committee within three weeks after the conclusion of each meeting.

15 Since the Certification Body is part of a public authority all Scheme Advisory Committee statements or advice regarding the Certification Body and the Scheme are recommendations. It is not mandatory for the Certification Body to follow the statements or advice of the Scheme Advisory Committee. However there are special procedures when advice is not followed (see 3.2 Actions when advice is not followed)

16 Any Scheme Advisory Committee statements, recommendations, or issuing of advice, requires that the matter under discussion have been announced in advance on the agenda.

17 Members with a direct interest in a specific certification, licensing, or other matter shall be excluded from voting relating to that matter.

18 Voting may be closed if requested by a member of the committee. The result of voting should be noted in the meeting minutes. As it is not mandatory for the Certification Body to comply with the recommendations from the Scheme Advisory Committee, there is no rule on how many votes are necessary to constitute a statement.

3.2 Actions when advice is not followed

19 If the Certification Body decides not to comply with the Scheme Advisory Committee's advice, the members of the Scheme Advisory Committee should consider to take appropriate action, which may include informing the Accreditation Body or other stakeholders.

20 The Management of the Certification Body shall document the reasoning behind the decision to not follow an advice from the Scheme Advisory Committee and shall maintain the document for review by appropriate personnel.

4 Responsibilities

4.1 Head of CSEC

21 The Head of CSEC is responsible for:

- ensuring that all members of the committee are fully aware that it is their responsibility to ensure the impartiality of the operations of the Certification Body and that there is a conclusion at the end of the meeting stating this
- setting up all matters relevant to the purpose of the Scheme Advisory Committee on the agenda
- reporting any decisions made during the interval between the meetings by the Scheme Advisory Committee (e.g., via e-mail discussions) at the next meeting and ensuring that these decisions are documented in the meeting minutes
- reporting changes in the Terms of Reference (this document) to the Accreditation Body
- providing to the Scheme Advisory Committee all documents necessary to fulfil the purpose of the Scheme Advisory Committee, as far as this does not conflict with the rules of the Scheme
- presenting to the Scheme Advisory Committee all major issues related to the operation of the Scheme
- reporting current Scheme matters to the Scheme Advisory Committee
- verifying the correctness of the meeting minutes
- ensuring the Scheme Advisory Committee's compliance to the rules described in this document

4.2 Secretary

22 The Secretary is responsible for taking notes at the meetings and documenting the discussions, decisions, advice, and comments from the meetings in protocols.

23 The Secretary does not vote at the Scheme Advisory Committee meetings.

4.3 Members

24 A member of the Scheme Advisory Committee commits to:

- Take active part in the stipulated tasks of the committee,
- Take active part in work groups and investigations,
- Be the contact for the committee towards its own organisation,
- Take appropriate action if the Certification Body decides not to comply with the Scheme Advisory Committee’s advice.

Appendix A Agenda for the SAC-meeting

25 Template agenda for SAC-meetings:

- Approval of the minutes from last meeting
- Membership matters
- Adaption of the draft agenda
- Emphasis on the members obligation to ensure the impartiality of the operations of the certification body and the members right to take actions when advice is not followed
- Report from activities by the CSEC since last meeting
- Proposed changes to the Scheme
- Changes to the Scheme
- Scheme policies
- Report from risk analysis
- CSEC matters regarding:
  - Licensing
  - Certification
  - Customer Satisfaction
  - Complaints
  - Appeals
  - Feedback from interested parties
- Common Criteria
- CCRA
- SOGIS
- Conclusion - Any matters that indicate that CSEC do not act impartial
- Provisional schedule for the next meeting