Dated: May 2015
Approved: September 2015
Version: 2.2

SOGIS logo	**SOG-IS Recognition Agreement Management Committee Policies and Procedures**

Document ID: JIWG-TOR-v2.2
Subject: JIWG Terms of Reference

General

1   In order to ensure the consistent application of the criteria and methods between SOG-IS Evaluation and Certification Schemes, a uniform interpretation of the currently applicable criteria and methods is needed.

2   In pursuit of this goal, the Participants of the SOG-IS Recognition Agreement [MRA] plan to conduct regular exchanges of information on interpretations and discussions necessary to resolve differences of interpretation. The Participants plan also to work on supporting documents concerning dedicated evaluation techniques like e.g. penetration methods or so-called Attack Methods, that shall be implemented by the CB claiming a Qualifying status for specific IT technical domains.

3   The SOG-IS Management Committee hereby establishes a so-called Joint Interpretation Working Group (JIWG).

Membership

4   The JIWG consists of Qualified Participants and additional discretionary Participants (on a voluntary basis) up to a numerical limit determined by the Management Committee.

5   In all cases shall the members be part of a governmental organisation representing a participant in the MRA.

Chairman

6   The Chairman of the JIWG is to be selected by the group from among the members and approved by the Management Committee. The chair is to serve for two years and is responsible for organising and moderation of the working group meetings and to coordinate with the Management Committee.

7   It is also the task of the chairman to have the SOG-IS website maintained and to authorize changes before they are made public.

Objectives

8   The main objectives of the JIWG is to provide technical advice and recommendations to the Management Committee, and to work on interpretations, on attack methods and to propose and work on new IT technical domains. The business of this Working Group includes:

   a) developing and recommending procedures for the conduct of the business of the MRA;

   b) recommending revisions of the MRA under the mandate of the MC;

   c) advising on the technical disagreements about the terms and application of the MRA;

   d) harmonising MRA scheme practices;

   e) developing and managing the JIWG supporting documents as to the background to interpretations and advising on any resultant decisions that could affect the application of either the criteria or methodology. This includes developing Attack methods for IT technical domains;

   f) proposing new IT technical domains and the assurance level and augmentations for which recognition can be claimed by the Qualified Participants;

   g) technical support to EU bodies developing regulations in this area.

Decisions

9   Each participant represented in the JIWG is to have one vote. Decisions about JIWG supporting documents for a specific IT technical domain and their publication shall be taken with a unanimous consensus by those participants representing a scheme that is qualified for that IT technical domain. All other decisions shall be taken by 2/3 majority voting.

Meetings

10   The JIWG usually meets four times a year. The meetings are hosted by the members on a rotating basis. The host nation will decide on the venue for the meeting and is responsible for the logistical support and writing of the minutes. The minutes of the meeting shall be distributed to the JIWG members and the Management Committee within one month after the meeting.

11   Every member can propose tasks to be treated in the working group. The tasks are executed with voluntary contributions from individual members and in a common effort during the meetings. Some tasks, if necessary, can be done in conjunction with a subgroup of experts mandated by the JIWG.

Support of technical work

12   Related to the task of developing and managing the JIWG supporting documents the JWIG might take the help of technical working subgroups (e.g. those dedicated to specific SOGIS Technical Domains).

13   A representative of the governmental part of the Qualified certification body or a technical expert who provides support to this CB) has to regularly attend the meetings of those work JIWG subgroup related to its recognition scope in order to:

   a) represent officially the CB in such a JIWG subgroup, i.e. the part of the CB taking the overall responsibility for the technical part of a certification

   b) ensure support the work of such JIWG subgroups by technical competence of the CB

c) enforce direct information flow from the JIWG subgroup into the CB (without biasing by a representative of a schemes commercial ITSEF or a related vendor as commercial organisation typically follow their specific own interests)

14   Qualified CB intends to regularly attend the meetings of those JIWG subgroups (at least 50 % of the meetings).

Documents

15   The JIWG issues documents to be part of the JIL. Public documents are usually made available through the SOG-IS website (or the Qualified Participants websites).

16   Sensitive documents issued by the JIWG can be distributed by the JIWG members to the following parties:

   a) Licensed labs from the schemes represented in JIWG.

   b) Members of the subgroups related to the specific IT technical domain.

   c) Sponsors/developers applying for a product evaluation/certification.

   d) Issuers accepting CC certifications as part of an approval process.

17   Each Qualified Participant can distribute a sensitive document according to these rules on his own discretion, without having to ask for a JIWG consensus.

18   Non-public documents like the original word formatted documents, meeting minutes, internal procedures, TORs, etc. are maintained by the chairman in a local repository. This repository is regularly exchanged between the JIWG members.

Duration

19   These Terms of Reference are valid from the date of approval by the Management Committee and are subject to review and modification at any time. Following a specific request for review and modification, the Management Committee will decide on the proposed modification.

References

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates Version 3.0