ISO SC27 WG3 Assurance Standards Review/Update (including ISO/IEC15408 and ISO/IEC18045)[1]

The SC27/WG3 managed call for input

Background

Both the CCDB and ISO SC27 WG3 are performing reviews concerning Common Criteria.

The purpose of this note is twofold:-

- To explain the background and how the two reviews differ but will be coordinated.
- To explain how to provide input for the SC27 WG3 assurance standards review process.

The roles of the two groups in this connection are outlined below:-

CCRA

The Common Criteria (parts 1,2, and 3 and the associated CEM) are kept under constant review by the Common Criteria Development, and Maintenance, Boards (CCDB and CCMB) and have been updated as a result of change requests via minor releases (currently at release 4, with another due shortly) and addenda.

See www.commoncriteriaportal.org/cc/ and www.commoncriteriaportal.org/cc/maintenance/ for more detail.

The documents have not, however, undergone a major review in almost 10 years, and, in many fields, technology, evaluation approaches, and end user needs, have all changed significantly since then. The recently updated CC Recognition Arrangement (CCRA), with its incorporation of collaborative protection profiles, is also leading to pressure for update in a number of areas as the iTCs start producing cPPs and their supporting documents and identify new assurance/process needs.

ISO

The CC/CEM documents are also published, in essentially[2] identical forms to the CCRA documents, by ISO as ISO/IEC15408 and ISO/IEC18045. The ISO group SC27/WG3 and the CCDB have worked together over the life of the current version to synchronise changes in new releases and ensure that the alignment continues.

The ISO review timetable now calls for the SC27/WG3 expert group to review these documents and SC27/WG3 has chosen to undertake this as part of a more wide ranging study period covering all of

1 Also known as CC and CEM

2 Mainly involving cosmetic/formatting changes

its role in assurance standards (NB not just ISO/IEC15408 and ISO/IEC18045).

Joint update

The CCDB is working with SC27/WG3, via liaison, aiming for updates to be performed jointly and in a harmonised way so that the current alignment remains effective. A variety of approaches will be used for this, including joint editors and/or joint editing sessions.

The Review Process

Inputs

ISO

SC27WG3 has issued a call for comments in respect of its wider assurance standards review via ISO national bodies. The study group terms of reference for this process are attached *here* and provide a more detailed background.

CCRA

The CCDB is taking input from three major routes:-

- All CCRA members are reviewing the documents,
- A number of iTCs are working on change proposals,
- The Common Criteria Portal web page (www.commoncriteriaportal.org) will be calling for inputs from the wider community.

Next Steps

ISO

The SC27WG3 call for input requests that these be submitted by 29 February 2016 to allow review by the working group at their next meeting (11-15 April 2016). The WG3 roadmap will then be updated, appropriate new work items identified, and relevant results of the study period used to facilitate the review of ISO/IEC 15408 and ISO/IEC 18045 and any subsequent update (in collaboration with CCDB).

CCRA

The CCDB has decided that all comments taken forward for consideration should have a CCRA member supporting them and that these comments should be in an actionable form (i.e. not only describing the issue raised but also indicating how this could be addressed) in text, pdf, or odf format (templates will be found shortly on the CC Portal (www.commoncriteriaportal.org)). The comments should be submitted by the 18th March in time for a preliminary discussion at the April CCDB meeting.

Scope

It is important to note that the input/comments can cover any aspects of IT product assurance. There is no limitation (to any notion of maximum 'EAL's for example).

Timescale

Both CCDB and ISO SC27/WG3 are currently seeking inputs for discussion at their respective next meetings. Following these discussions and subsequent liaison concerning best routes for collaboration, it will be possible to provide details of the next stages and timeframes. The current CCDB outline plans however anticipate a 12 month update process, trials against changes, and then a gradual transition to the new standard.

How to submit Comments to the SC27 WG3 Rapporteurs

ISO has a well defined commenting process using national standards bodies and this is being used as the primary input route.

The SC27 WG3 rapporteurs[3] have however, also created this discussion forum to allow for more informal discussion/input from CCUF members.

The rapporteurs are seeking contributions on the topics listed in the Study Period TORs - clearly indicating the responder viewpoint (e.g. developer, end user, certification body, security consultant, etc.), and backed, where possible with clear argument/evidence.

NOTE This is a public commenting process: the text of comments and responses may be distributed, or made available in other ways during the process, without restriction.

Helpful Questions

I am still confused – tell me again, why are there two reviews?

CCDB and ISO have distinct responsibilities, the CCDB is responsible for the CC and CEM that is the foundation of the CCRA recognition arrangement, while ISO SC27 WG3 manages the related international standards ISO/IEC 15408 and ISO/IEC 18045. Both groups work together and aim to keep these in line. The SC27 WG3 review however is significantly wider in scope. It is asking for responses concerning all aspects of IT security assurance evaluation, where CC fits in, how developers/end users/policy makers/others see the overall landscape, etc.

So which one should I respond to?

If your response concerns wider aspects and not just the detail of CC/CEM then the ISO review is where you should feed your comments (ideally through your ISO National Body). If you are commenting directly on the CC or CEM (ISO/IEC 15408 or ISO/IEC 18045) then you could use either the ISO route or CCDB route.

How long do I have to respond?

To allow initial reviews of the quantity and key themes of comments at their next meetings, ISO SC27WG3 have set a deadline of 29 February 2016 and the CCDB have a deadline of 18th March.

---

3 David Martin*, Fiona Pattinson*, Helmut Kurth*, Jean-Pierre Quemard, Dietmar Bremser (those marked with * can be found on the CCUF site)

How do I provide input?

The simplest and preferred route for ISO is via the relevant ISO national bodies. A less formal alternative is via posting/discussion here as the SC27 WG3 Rapporteurs will also use this as input in their reporting.

The CCDB input process is described briefly above and more detail will be provided on the CC portal.