Common Criteria in the Cloud Technical Community Terms of Reference

Table of Contents

1. Identification

Name: Common Criteria in the Cloud Technical Community Terms of Reference

Version: 1.0

Date: 5 December 2023

Technical Community: Common Criteria in the Cloud

Technical Community Abbreviation: Cloud-TC

2. Technology Area and Scope

The scope of this Technical Community (TC) are products and services utilizing a cloud platform or environment.

The Cloud-TC will develop evaluation collateral and guidance to extend CC evaluations into cloud scenarios.

The initial aim is to consider the Essential Security Requirements (ESR) [1]. It is anticipated that the scope of the first version of any work products is limited to solve the security problem as defined in the ESR in order to be completed in a timely manner. After the completion of the first collection of work products, associated Supporting Documents, the Cloud-TC may consider to expanding the scope of subsequent works.

3. Key Persons / Affiliations

Key roles are defined in Section 7, "Roles".

4. Collaboration Infrastructure

To enable collaboration, the Cloud-TC uses collaboration services including email notification, discussion forums, and file storage that are accessible to Cloud-TC members.

The Cloud-TC is using a combination of hosted collaboration services provided by the Common Criteria Users Forum and GitHub.

5. TC Development Process

5.1. Application of the White Paper

This Cloud-TC follows the processes defined in Establishing Technical Communities and Developing Collaborative Protection Profiles [3] with the version agreed with the CCDB Liaison. The version should normally be the latest version approved by the CCRA CCDB Cloud-TC or the CCRA CCDB as applicable.

5.2. Maintenance

The Cloud-TC remains in place to answer inquiries and update the work products as may be requested by CCDB, Cloud-TC members and/or others stakeholders. The Cloud-TC Chair is responsible for establishing an appropriate periodic schedule and organizing the Cloud-TC to review, and if needed, update the TC work products.

6. Policies

6.1. Membership

This TC is open to all interested persons who have an active role in this technology area and in CC evaluation. To join the TC, each must submit an application located here.

6.2. Principles

The Cloud-TC should be working in manners that promote fair competition and meet the six principles of international standardization determined by the WTO-TBT. See G/TBT/1/Rev.15 (24 September 2019) "DECISIONS AND RECOMMENDATIONS ADOPTED BY THE WTO COMMITTEE ON TECHNICAL BARRIERS TO TRADE SINCE 1 JANUARY 1995" [5] or later revision.

- Transparency
- Openness
- Impartiality & Consensus
- Effectiveness & Relevance
- Coherence
- Development Dimension

If the Cloud-TC finds any of the principles not to be appropriate, it should inform the CCDB via the Liaison on what exceptions would be required.

6.3. Code of Conduct

The Cloud-TC draws from the ISO Code of Conduct for the technical Work [4] and the Contributor Covenant Code of Conduct [6].

Work for the net benefit of the international community	We recognize that the development of collaborative Protection Profiles is for the net benefit of the international community, over and above the interests of any individual or organization. We are committed to advancing collaborative Protection Profiles within their agreed scope and we will not hinder their development.

Uphold consensus and governance	We will uphold the key principles of International Standardization in the creation of collaborative Protection Profiles: consensus, transparency, openness, impartiality, effectiveness, relevance, coherence and the development dimension.
Agree to a clear purpose and scope	We are committed to having a clear purpose, scope, objectives, and plan to ensure the timely development of collaborative Protection Profiles.
Participate actively and manage effective representation	We agree to actively participate in standards development projects. We will make our contributions to the work through the agreed upon tools and procedures in accordance with the TC guidance documents.
Escalate and resolve disputes	We will identify and escalate disputes in a timely manner to ensure rapid resolution. We will uphold the agreed dispute resolution processes.
Behave ethically	We will act in good faith and with due care and diligence. We will avoid collusive or anti-competitive behavior. We will promote a culture of fair and ethical behavior.
Follow a Code of Conduct	We are committed to following a code of conduct in an open, welcoming and inclusive manner. In meetings we are committed to: • conducting ourselves in a professional manner • respecting others and their opinions • accepting group decisions • ensuring that the views of all (including those whose first language is not that of the meeting) are heard and understood

6.4. Language

The Cloud-TC work and documents will be executed in the English language.

6.5. Revision of the Terms-of-Reference

The ToR should be subject for discussion and revision as needed and agreed upon within the Cloud-TC.

The CCDB should be informed via the CCDB Liaison whenever changes are made to the ToR that are principal in nature and may affect the endorsement status of the Cloud-TC within the CCRA.

6.6. Decision-making

6.6.1. Editorial decisions

Editorial decisions (including correction of technical inconsistencies) are made at the discretion of the Technical Editor, in consultation with the Core SMEs and Cloud-TC Chair when needed.

6.6.2. Technical decisions

Ideally, technical decisions are made by reaching group consensus (see Section 6.7, "Voting" for a definition). In most cases, the Core SMEs will be able to propose a resolution that is acceptable to the Cloud-TC and the originator of the issue.

As a guideline, decisions are made according to the following process:

- Major Decisions shall be made via the TC collaboration tools in github. The Cloud-TC will provide one or two weeks to make the decision. Minor decisions, such as regular commitments to draft TC documents, may be made by acclimation during scheduled TC meetings.
- Consensus is the default and strongly preferred method for resolution. However, if after a month consensus cannot be reached for a particular issue, then voting should be implemented.
- If there are members that disagree with a decision, they can request the reason for objection to be documented by Cloud-TC Management.
- Once a decision has been made by the group it will be adopted and implemented. However, as a means to change direction or scope, any member can try to build a consensus for reversing a prior decision.

Other Cloud-TC members are encouraged to post comments in response to issues and proposed resolutions at any time.

A typical issue should be resolved within a two week period. Some issues may require more time for study and deliberation or due to holidays or other events.

6.7. Voting

Decisions shall be taken based on of the consensus principle whenever possible.

> Consensus: General agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments.
>
> NOTE Consensus need not imply unanimity.
>
> — ISO/IEC Guide 2:2004

The Cloud-TC may define different classes of voting, but for votes related to the TC itself, the process here defines how the voting will proceed. If the class of vote needed has not been defined, then the

process here will be used by default.

Voting is used infrequently to formally decide on a particular TC issue. The following would be considered TC issues to require a formal vote:

- Establishing formal working groups within the TC (such as the Interpretation Team or special interest groups to work on specific areas)
- Changes to the TC governing documents (such as the Essential Security Requirements or Terms of Reference)
- Public Review/Release of documents

As determined by the TC, additional voting classes will be defined in the documents where they will be used.

6.7.1. Vote Eligibility

Voting is limited specifically to the members defined at the time the vote is called. Membership in the Cloud-TC is defined as inclusion on the Cloud-TC roster on the CCUF approved collaboration tool.

One vote is allowed for each member organization, not for each individual member, regardless of membership within the Cloud-TC. *Organization* is defined according to the definition adopted by the CCUF; for commercial enterprises, a parent company and all of its divisions and subsidiaries comprise one organization. It is the responsibility of each organization to determine which individual member will cast a vote on its behalf.

Eligible voting organizations are determined at the time the Call for Votes is sent out based on inclusion on the Cloud-TC mailing list. Any organization not included on this list at the time the Call for Votes is posted is ineligible to cast a vote.

6.7.2. Vote Workflow

As a guideline, voting takes place according to the following process:

1. A Call for Votes is posted, including the mechanism for casting ballots and time period during which ballots are accepted
2. At the end of the voting period, ballots are tabulated and reviewed by the designated ballot officer.
3. Results of voting are posted, including a summary of the vote and the votes cast by each organization.

This process is illustrated, below. Timing for each part of the process is provided as a benchmark. A typical voting cycle should be completed within a three-week period. Some voting periods may be longer due to holidays or other events.
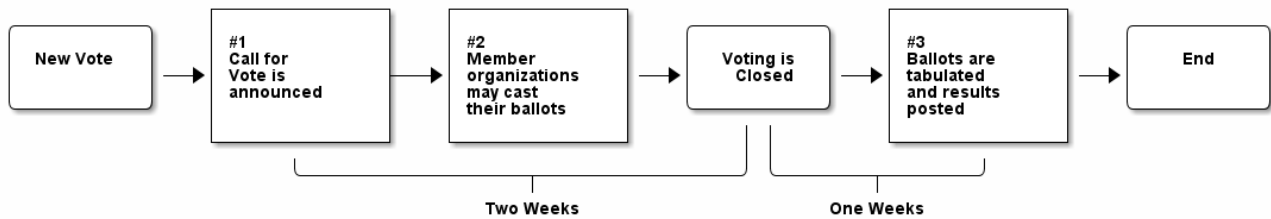
Figure 1. Vote Workflow

Votes submitted shall be explicit: positive, negative, or abstention. A positive vote may be accompanied by editorial or technical comments, on the understanding that the TC Chair or Technical Editor (as applicable) will decide how to deal with them. If a voting member finds the proposal unacceptable, it shall vote negatively and state the technical reasons. It may indicate that the acceptance of specified technical modifications will change its negative vote to one of approval, but it shall not cast an affirmative vote which is conditional on the acceptance of modifications.

6.7.3. Vote Counting

A vote is approved if:

- A two-thirds majority of the Counted votes of the Cloud-TC are positive.
- At least five votes are cast.
- For elections of TC roles, only a simple majority is required when voting is needed.

Counted votes are determined by the following conditions:

- Only one vote per organization is made.
- Negative votes concerning technical issues are encouraged to provide a rationale.

> An organization submitting multiple non-matching votes is allowed to determine the final vote to be counted before voting is closed. The onus is on the organization to ensure the proper vote. A set of non-matching votes will cause the organization votes to not be considered Counted votes.

Abstentions are not Counted votes in the final total. They will be noted in the record only.

6.8. Meetings

Meetings are held at times, with frequency, and in forms that are determined by the Cloud-TC members.

6.9. Record-keeping

The following records are created and maintained:

- Meeting attendance and summary of decisions
- Action items and their disposition

- Comments and resolutions

- Interim draft documents

- TC Roster with indication of voting members

- Key persons and affiliations

These records are accessible to Cloud-TC members.

6.10. Patent and other intellectual property

6.10.1. Essential patents

Essential Patent means any issued or pending patent claim for which its use is necessary (i.e., there is no commercially and technically feasible non-infringing alternative) to fulfill the conformance requirements of the work product(s) including, but not limited to, guidance for cPP and SD authors produced by the Cloud-TC.

Cloud-TC members must inform the Chairperson if they are personally aware of any potential Essential Patent, regardless of the owner or controller of such patents.

As soon as an Essential Patent is identified, the Cloud-TC should seek resolution in the following priority order:

- The owner of the Essential Patent grants a license, on reciprocally reasonable and non-discriminatory terms and conditions, to anyone desiring to manufacture, sell, or otherwise employ products conforming to the workproduct(s); or,

- If the owner of the Essential Patent is unwilling or unable to grant such a license, then the Cloud-TC should modify the work product(s) so as not to infringe on the Essential Patent.

6.10.2. Members intellectual property

Cloud-TC members are solely responsible for protecting their organization's proprietary, trade secret, or other sensitive information. The Chairperson, other members, and the technical infrastructure used by the Cloud-TC, do not provide any assurance of such protection.

6.10.3. Work product ownership

No copyrights will be asserted on Cloud-TC work products. Cloud-TC members may use such work products but may not assert moral or authorship rights. The use of those work products is controlled by the Common Criteria evaluation process: claims of conformance to the work products are meaningless without Common Criteria certification.

6.11. Inappropriate topics

TC members should not discuss topics that could be interpreted as collusion, such as pricing, licensing terms, territories, market shares, or litigation. Cloud-TC members are encouraged to inform the Chairperson if they become aware of such discussions.

6.12. Common Criteria considerations

The work products of this Cloud-TC intend to conform to CCRA requirements for mutual recognition.

Further considerations, such as CC/CEM conformance and other mutual recognition schemes are to be determined.

7. Roles

7.1. Chairperson(s)

Chairpersons oversee the operation of the Cloud-TC in accordance with the ToR: assign or approve key persons, set and manage schedules, convene meetings, plan and lead activities, solicit participation and input, manage issues and discussions. Chairpersons can also work as core SMEs and make comments or vote on any technical issues. However comments or vote from chairpersons are treated equally and any decision-making should be done as described at Section 6.6, "Decision-making".

Every 12 months, or when necessary due to vacancies, or when so requested by members of the Cloud-TC, the Cloud-TC Chair should discuss the current assignments of key persons with the Cloud-TC membership.

7.2. ISO Liaison

The ISO Liaison is a role that interacts and is responsible for communications and deliverables with the ISO/IEC 15408, ISO/IEC 18045, SC 27 WG 3 groups.

7.3. Record Manager

The record manager is a role that primarily supports the Cloud-TC Chair. Unless agreed otherwise with the Cloud-TC Chair, the responsibilities include:

- Establish and maintain a record with key persons and their affiliations.
- Establish and maintain an updated roster, including identity of organisations/nations eligible to vote.
- Administrate membership applications.
- Keep mailing lists up to date.
- Provide access for new members to appropriate Cloud-TC resources.
- Make notes of meetings.
- Keep the Cloud-TC action item list updated.
- Ensure that Cloud-TC records are maintained, available and in good order.
- Support the Cloud-TC Chair in daily operation of the Cloud-TC.

7.4. Technical Editor(s)

Technical Editors serve as the primary author for the TC work products: create and update documents to reflect the decisions of the Cloud-TC, post drafts for access by Cloud-TC members, and finalize drafts for approval.

7.5. Core SMEs

Core Subject Matter Experts comprise a team that develops the initial drafts of cPPs and SDs, evaluates issues and comments, and proposes appropriate and equitable resolutions to the Cloud-TC. The Core SME team is composed of a balance of industry, end user, and Common Criteria experts who can work effectively with the rest of the Cloud-TC members. Core SMEs should have adequate competence, time and resources available in order to contribute to provide timely resolutions to the Cloud-TC.

7.5.1. Industry SMEs

Industry SMEs provide knowledge of the technology area and experience with product evaluation. They also help make appropriate decisions based on their practical knowledge of markets, customer expectations, implementation, and costs.

7.5.2. Lab SMEs

Lab SMEs provide a solid understanding the evaluation process in the various schemes under the CCRA, and can offer contributions from a unique perspective. They can offer perspective on evaluation activities (what the evaluator does to test or otherwise confirm compliance with requirements), and well as ensuring the requirements are written in such a way that there can be a clear pass/fail criteria.

7.5.3. Certification Body SMEs

Common Criteria certification bodies provide knowledge and experience in the expression of functional and assurance requirements in the language of the CC, and help ensure that the cPP and SDs comply with CCRA-accepted standards and practices.

7.5.4. Other SMEs

Other SMEs can come from a wide range of background, including government technical experts, end user representatives, as well as consultants or those from academia.

8. References

- [1] Common Criteria in the Cloud Essential Security Requirements, Online (https://github.com/CC-in-the-Cloud/Admin/blob/Working/ESR/CC_in_the_Cloud_ESR.pdf)
- [2] Common Criteria in the Cloud Technical Community - Key Persons and Affiliations, Online (link when available)

- [3] Establishing International Technical Communities and collaborative Protection Profiles development, Online

- [4] ISO CODE OF CONDUCT FOR THE TECHNICAL WORK, Online

- [5] DECISIONS AND RECOMMENDATIONS ADOPTED BY THE WTO COMMITTEE ON TECHNICAL BARRIERS TO TRADE SINCE 1 JANUARY 1995, Online Search

- [6] Contributor Covenant Code of Conduct, Online