EUCC ISAC

CC Framework for Embedded AI (CCFAI)

EU Common Criteria Information Sharing and Analysis Centre

Terms of Reference (TOR)

V1.1 - May 2026

Traffic Light Protocol (TLP) Classification

TLP Level	Description	Sharing Scope
TLP:CLEAR	Disclosure is not restricted.	May be shared freely and published without limitation.

Table of Contents

1. Introduction

The EUCC ISAC is a non-for-profit association governed by Belgium law, CC Framework for embedded AI (CCFAI) is a technical group of the EUCC ISAC. Terms of Reference provide practicalities, details and procedure in relation with the working of CCFAI which are not specified by the statutes of the EUCC ISAC.

CCFAI addresses the concerns of vendors, ITSEFs, national schemes and regulators related to the adaptation and extension of Common Criteria (CC)-based evaluation and certification to AI-enabled systems, with a specific focus on embedded AI. AI-based technologies are increasingly integrated into products and services that impact everyday life; beyond large language models and chatbots, many critical systems rely on machine learning components. Ensuring their cybersecurity, robustness, and trustworthiness is becoming a day-to-day challenge. CCFAI also structures information sharing on AI-specific cyber threats, in support of the EU's cybersecurity and AI policy objectives, and brings together Members that share the same values about high-level security evaluation approaches and agree to the rules of collaboration.

CCFAI aims to bring harmonization added value at the intersection of the Common Criteria (ISO/IEC 15408) and emerging AI cybersecurity requirements, in alignment with the European goals defined under the Cybersecurity Act (CSA) and the EU AI Act. The harmonization work at CCFAI is essential to ensure that ITSEFs apply equivalent methods and evaluations to AI-enabled Targets of Evaluation . This is crucial for the mutual acknowledgement of certificates coming from other participating certification countries and/or schemes.

The mission is that all participants gain an agreed common understanding of how Common Criteria evaluation and certification methodologies shall be adapted, extended and applied to AI-enabled products, with a particular emphasis on embedded AI systems.

In recent years, Security Evaluation standards and the AI cybersecurity landscape have evolved in several directions:

- Expanding diversity of AI paradigms and form factors (embedded models, cloud-based services, LLMs, computer vision systems, etc.), each with very different attack surfaces and safeguards;
- Emergence of AI-enabled products in critical markets with shorter development cycles and heterogeneous levels of security assurance (from industrial and automotive to medical, mobile, and IoT devices embedding machine learning components);
- Emergence of parallel international initiatives aiming to define AI security evaluation methodologies, with no single dominant framework established yet;
- Evolution of CCRA and its interaction with AI-specific evaluation needs;
- Evolution of European cybersecurity regulations, notably the EU AI Act, NIS2 and the Cybersecurity Act (CSA).

In this context, CCFAI targets a European and, where relevant, international harmonization of methodology for the evaluation and certification of AI-enabled products under the Common Criteria framework, with a particular emphasis on embedded AI. New analysis methods addressing AI-specific properties – such as data integrity and provenance, model confidentiality, robustness to adversarial examples, and the secure lifecycle of AI components – are to be evaluated throughout all participating evaluation and certification schemes. CCFAI's mission is that all participants apply the same understanding of how Common Criteria concepts (TOE, assumptions, threats, SFRs, SARs, attack potential, etc.) should be interpreted and extended for AI components. This is fundamental for the mutual acceptance of certificates among the participating schemes and countries. For this reason, the group consists of certification bodies and authorities, accredited evaluation laboratories (ITSEFs), AI and

cybersecurity vendors, and end-user organisations with a legitimate interest in the evaluation of AI-enabled products.

This group is driven by the vendors and schemes and has no educational mission.

The CCFAI collaboration is conformant with European antitrust laws as it is managed as an ISAC subgroup under the ISAC antitrust bylaws.

This document contains the mission statement, organization and functioning rules for this subgroup.

The compliance to ToR by each CCFAI Member is required to preserve each Member's sensitive assets, guarantee the trustworthiness in the subgroup exchanges and enable CCFAI productivity. It is essential that CCFAI Members share the same values and work towards agreed shared objectives.

2. Guiding principles

CCFAI is led by voluntary consensus principles in accordance with the following attributes:

- Openness – the procedures or processes used for creation, revision, reaffirmation, and withdrawal of CCFAI's technical documents are transparent and open to all the Members. CCFAI's Members are provided meaningful opportunities to participate in the definition of the technical documents on a non-discriminatory basis.
- Balance and Lack of Dominance – CCFAI's decision making process, and the development of deliverables should be balanced; there should be meaningful involvement from a broad range of parties, with no single interest dominating the decision-making.
- Due Process – due process shall include procedures, adequate notice of meetings and documentation development, a defined adequate period to review drafts and prepare views and objections, access to views and objections of other participants, within the limits imposed by the confidentiality of information and the strict respect of the antitrust compliance guidelines.
- Procedural Appeals – an appeal process shall be available for the impartial handling of procedural appeals.
- Consensus – consensus is the rule (general agreement, but not necessarily unanimity); during the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes. To validate this general agreement, votes can be organised pursuant to the following CCFAI's Terms of Reference (ToR).

3. Mission and powers

The mission of CCFAI is to adapt and extend Common Criteria (CC)-based evaluation and certification to AI-enabled systems, with a particular emphasis on embedded AI, and to structure information sharing on AI-specific cyber threats, in support of the EU's cybersecurity and AI policy objectives. CCFAI is therefore tasked with:

Due to the diversity of AI technologies and use cases, defining a precise scope for AI cybersecurity is inherently challenging:

- "AI systems" cover a wide range of paradigms (embedded models, cloud-based services, LLMs, vision systems, etc.) with very different attack surfaces and safeguards.
- the field of AI Security Evaluation is still in its methodological infancy, with many parallel initiatives and no single dominant framework;

- stakeholders (manufacturers, ITSEFs, national schemes, regulators) have heterogeneous needs, especially regarding certification and evaluation depth.

Considering these constraints, the subgroup adopts a dual scope:

1. Workstream 1 – CC Environment for AI Security: designing a CC-based environment for AI cybersecurity evaluation and certification, aligned with the CEN/CLC JTC21 WG5 harmonized standard on AI Cybersecurity Requirements and related international standards. This includes mapping AI cybersecurity requirements into CC concepts (TOE definition, assumptions, threats, SFRs, SARs), identifying gaps of CC as applied to AI-enabled products, proposing extensions or extended SFRs fully compatible with ISO/IEC 15408 (CC) and ISO/IEC 18045 (CEM), progressively structuring a Protection Profile (PP) or PP modules for embedded AI under EUCC, without altering their core concepts, and providing AI-specific input to the minimum ITSEF requirements for security evaluations of software, in coordination with the EUCC ISAC Software Technical Group.
2. Workstream 2 – Information Sharing on AI Cybersecurity: structuring the collection, analysis and sharing of AI-specific attack paths and vulnerabilities in embedded AI systems (e.g. adversarial examples, data poisoning, model extraction, backdooring), developing attack methods and an attack catalogue that may support ITSEFs in assessing embedded AI systems, contributing to the application of attack potential to AI-specific attacks, and exploring mechanisms for coordinated vulnerability disclosure, in close cooperation with ENISA, relevant communities and standardization bodies.

4. Membership

Members of CCFAI are members of the EUCC ISAC and shall follow its Statutes. Membership to CCFAI is open to those EUCC ISAC Members who meet the criteria set out in Article 6 of the EUCC ISAC Statutes as complemented by Terms of Reference.

CCFAI membership is made of:

4.1. Executive members with voting rights:

a. National Cybersecurity Certification Authorities (NCCAs) and Conformity Assessment Bodies (CABs) operated by a NCCA involved in the EUCC Subgroup on EUCC maintenance (EsEm);

b. National Accreditation Bodies (NABs);

c. Manufacturers and Providers of ICT products that have relevant and recent products within the last 3 years evaluated in Europe by a CAB under the EUCC Scheme and that expressed sufficient and motivated interests in EUCC;

d. CABs that are not operated by an NCCA, accredited under the Cybersecurity certification framework by a qualified NAB – whether they act or not on behalf of a NCCA.

e. Labs and Information Technology Security Evaluation Facilities (Labs/ITSEFs) that operate within the European Union and whose application is supported by an NCCA.

f. End-user group or an organisation contributing to the development or using the EUCC Scheme certified products (e.g. Payment schemes, Telco's, trade associations etc.) and which have a significant part of their business in Europe.

4.2. Associate Members with no voting right:

a. One or several representatives of ECCG subgroup for EUCC maintenance and review (EsEm);
b. NCCAs or CABs operated by an NCCA involved in the EsEm;
c. National Accreditation Bodies (NABs);

4.3. Observers:

a. Cybersecurity certification authority operating outside the European Union;
b. Non-European consortium made of laboratories, conformity assessment bodies, vendors and led by a third-country national cybersecurity certification authority.

Membership shall fulfil criteria and admission process pursuant to the chapter two of the EUCC ISAC Statutes.

4.4. Membership in Trial Status

Manufacturers or Providers of ICT products that have not yet completed an evaluation or certification under the EUCC but have demonstrated sufficient interest and commitment to EUCC topics

4.5. Historic Members

In accordance with Article 9 of the Statutes of the EUCC ISAC, CCFAI (CC Framework for Embedded AI) is established as a Technical Group within the EUCC ISAC. As CCFAI is a newly constituted Technical Group, this section applies only to organisations that were present in the ISCI Subgroup CC Framework for embedded AI.

Organisations that were, as of 20 April 2026, members of the CCFAI ISCI Subgroup (as a subgroup of ISCI) are recognised as Historic Members under Article 9 of the EUCC ISAC Statutes. These organisations, or their designated senior representatives, shall have the right to become Members of the Association without any membership assessment or admission procedure. Upon notification of their application in accordance with Article 9 of the EUCC ISAC Statutes, such Historic Members automatically become Members of the EUCC ISAC and CCFAI.

5. Liaisons

CCFAI may request the Steering Committee to establish transient or permanent liaison with any other entities. To this end, CCFAI defines the conditions of participation and the content of the liaison statement to be submitted to the Steering Committee for approval pursuant to article 23 of the EUCC ISAC Statutes.

In particular, CCFAI plans to establish and maintain liaisons with the following bodies and communities, whose work is directly relevant to the subgroup's mission:

- CEN/CLC JTC21 WG5, to ensure alignment with the harmonized AI cybersecurity standard and its implementation in European schemes (including the EU AI Act);
- CEN/CLC JTC21 WG4, to ensure alignment with the harmonized AI trustworthiness framework and its implementation in European schemes (including the EU AI Act);
- ISO/IEC JTC1 SC27/WG3, in particular on ISO/IEC NP 26160 (augmenting the ISO/IEC 15408 series with AI-specific functional requirements and evaluation guidance) and ISO/IEC NP 25959

(application of attack potential to deep learning-based technology), with a cyclical exchange between CCFAI findings and these standards;

- ISO/IEC / JTC 1/ SC42 /WG3 on AI reliability and robustness;
- ENISA, to support state-of-the-art (SoTA) documentation on AI cybersecurity and to use EUCC as a structuring framework promoting safe and trustworthy AI systems within the Union;
- the ECCG subgroup for EUCC maintenance (EsEm) and other EUCC ISAC Technical Groups, to ensure consistency of CCFAI deliverables with the broader EUCC framework;
- open or semi-open communities cataloguing AI vulnerabilities and mitigations, in particular the OWASP AI Exchange, for the bidirectional sharing of relevant insights on AI-specific attack paths and defences.

6. Other conditions specific to the group

Information discussed in the meetings or communicated in the reports is considered confidential and treated as such. CCFAI discussions shall be free without suppressing opinions and meanings:

- Conflicts shall be discussed on technical level only,
- Individual business and other interests are not subject of CCFAI discussions,
- Carrying out competitive relations by discrediting or denigrating other Members or influencing others against a certain Member, is strictly contrary to the principles of collaboration within CCFAI. Such behaviour shall be immediately addressed and stopped by the Chairman and leads to the application of penalty: activating the *Non-Compliance and Exclusion Procedure* as defined in Article 10 of the TOR.
- The information discussed in the meetings or communicated in the documents may not be used for commercial activities other than the intended mission of CCFAI.

Each Member can provide topics to the Chair, Vice-Chair for the agenda any time prior to a meeting.

- Whether a topic could be managed in the next meeting is a matter of time remaining prior to the meeting and of remaining meeting time of an already given agenda.
- The chair cannot guarantee that a late topic is included in the next meeting, but if not, it shall be a part of the agenda of one of the next meetings. Its urgency can be discussed in the plenary.

The collaboration using electronic media shall be based on the CCFAI repository for upload and download.

The CCFAI repository keeps a database of

- Meeting minutes,
- Presentations held.
- Participants being in the trial period (MITS) gain access when they become acting Members.

7. Applications

Applications are subjected to a validation procedure by CCFAI and inform the Steering Committee of the EUCC ISAC.

CCFAI defines here the application process within its group in accordance with the criteria as set out in article 6 on Membership of the EUCC ISAC Status:

Application requests should be supported through an existing member or the Chairman of CCFAI. The member must write an email requesting membership, the email must contain, Company/Organization name, proposed attendee, details of organization, and experience with CC certification.

Each organization agrees by signing in as a member to the rules described in CCFAI ToR described in this document. Applications from an authorized CB will follow a different process and have to be submitted to the chair of the ISAC Steering Committee.

The members should represent a spectrum as wide as possible of the parties involved in the evaluation and certification of AI-enabled products, with a specific emphasis on embedded AI. The main groups identified so far are AI vendors and integrators, hardware and software vendors providing AI-enabled components, certification bodies (NCCAs/CABs), IT security evaluation facilities (ITSEFs/laboratories), service providers, and end-user organisations relying on certified AI components.

The acceptance criteria for new member application are based on the following main paradigms that are CCFAI specific:

1. Applicant profile, technical skills and competence
2. Motivation/Reciprocity Benefit
3. Acceptance of CCFAI rules for collaboration
4. Acceptance of CCFAI results for their own evaluation, respectively certification

Applicant profile, technical skills and competence

The new applicant is expected to provide a comprehensive presentation of its entity:

- Entity status: vendor, laboratory
- Organization, regional origin, business profile, link to other company/schemes/University
- Related product and markets,
- Entity experience in the domain:
  - Artificial Intelligence
  - Software and Hardware Cybersecurity
  - Security certification/ used certification schemes…
  - Confidentiality management
- Entity representative for CCFAI (member expertise and experience, technical publications)
- Sponsorship from an existing CCFAI member
- The request email will be processed by the Chairman/Vice-chair.
- An invite to the applicant to present at the next full meeting will be delivered within 2 calendar weeks.
- During this meeting the applicant is expected to give a presentation detailing its organization and his relationship to Common Criteria Certifications.
- The Chairman or the Vice-chair will ask the members via e-mail if there are any concerns with the applicant’s request.
- The period for replying to this membership request is 2 calendar weeks.
- After a period of 2 weeks the Chairman will
  - Contact the applicant to confirm or deny membership.

- Inform the Steering Committee about the decision of CCFAI.

Objectives:

Assess the trustworthiness of the entity and the relevance to CCFAI discussion. Avoid malicious members.

Metrics:

Elements to be provided by the applicant:

- Guarantees provided by the member to ensure information confidentiality.
- Demonstrated skills and experience enabling an active contribution to CCFAI topics.

Examples of acceptable (non-exhaustive) evidence:

- Evidence of Common Criteria (CC) evaluation activity within the EUCC scheme (at least initiated).
- Past or ongoing CC evaluations of AI-enabled TOEs, or documented experience in evaluating AI cybersecurity properties (robustness, data integrity, model confidentiality, secure lifecycle of AI components).
- Members to provide evidence of interest and competence in security evaluations of AI-enabled products, at the assurance levels relevant to the EUCC scheme (Substantial and/or High), including exposure to AI-specific threats such as adversarial examples, data poisoning, model extraction or backdooring.
- Experience with, or commitment to contribute to, CC evaluations of AI-enabled TOEs, including where applicable forthcoming CCFAI-related Protection Profiles or PP modules for embedded AI, and alignment with the CEN/CLC JTC21 WG5 harmonized standard on AI Cybersecurity Requirements.

Additional requirements/metrics:

- Conform to the “Minimum ITSEF Requirements for security evaluations of AI-enabled software/hardware” once defined by CCFAI (optional, for lab applicants).

Motivation / Reciprocal benefit

- Applicants have to declare how they intend to contribute to CCFAI and for what purpose.

Objectives:

- Ensure an active and valuable contribution to CCFAI,
- Check reciprocal benefit of applicant and CCFAI,
- Check recognition of CCFAI works,
- Show long term interest about high-level security evaluation approach,
- Discard applicants that would not or could not participate actively to the CCFAI Technical Group or that are interested by a short-term participation.

Membership in Trial Status (MITS):

CCFAI may grant a Membership in Trial Status (MITS) to Manufacturers or Providers of ICT products that have not yet completed an evaluation or certification under the EUCC scheme but have demonstrated sufficient interest and commitment to EUCC topics, in accordance with Article 9.6 of the Articles of Association of the EUCC ISAC.

MITS members are invited to attend CCFAI meetings and may actively participate and contribute to CCFAI activities, without voting rights.

CCFAI shall reassess each MITS after a period of one (1) year from the date of admission.

- If the certification conditions listed in Article 6 of the EUCC ISAC Statutes and the Members' obligations listed in Article 6 of the CCFAI Terms of Reference (ToR) are fulfilled, the MITS shall be considered an Executive Member with voting rights.
- If the certification conditions listed in Article 6 of the EUCC ISAC Statutes are not yet fulfilled, whereas the Members' obligations listed in Article 6 of the CCFAI ToR are fulfilled, the MITS period may be extended for an additional one (1) year, upon decision of CCFAI Members following the voting rules laid down in Article 9 of the CCFAI ToR.

After the MITS extension period, if the certification conditions listed in Article 6 of the EUCC ISAC Statutes remain unfulfilled while the Members' obligations listed in Article 6 of the CCFAI ToR continue to be fulfilled:

- CCFAI Members may decide to exclude the MITS following the voting rules laid down in Article 9 of the CCFAI ToR,
- or the EUCC ISAC Steering Committee or CCFAI may vote to grant a derogation in accordance with Article 11 of the EUCC ISAC Statutes.

In all cases, the decision and status of the MITS - including any conversion, extension, exclusion, or derogation - shall be formally communicated to the EUCC ISAC Steering Committee.

8. Members obligations

It is expected that all Members work actively towards the goals of CCFAI. This can take various forms such as regularly participating in the meetings.

It is discouraged to be merely an entry in the CCFAI e-mail distribution list, and membership status may be under review by CCFAI. Normal consensus rules apply here.

CCFAI will hold at least two (2) physical meetings per calendar year, complemented by regular online meetings (typically at least one per month) to ensure continuous progress on deliverables.

Members are expected to physically attend at least one (1) of the two (2) physical meetings held in a calendar year (i.e. 50% minimal physical attendance), and to actively participate in the online meetings.

The chair will record attendance to all meetings, physical and virtual, where attendance has dropped below the expected minimum, a discussion will take place to the future involvement of the individual party due to lack of interest/participation.

Members are expected to participate, in at least one of the following tasks:

- Participation in at least one sub-group or task
- Generating documents
- Editing documents
- Commenting and reviewing documents

It is not expected that Members fulfil all the items above, but a reasonable subset is expected.

Members should be courteous to other Members, aggressive behaviour or disrespecting behaviour should be reported to the Chair.

9. Non-Compliance and Exclusion Procedure

In the event that an CCFAI Member does not comply with the EUCC ISAC Statutes, the EUCC Terms of Reference (ToR), or any of their annexes, the CCFAI Chairman shall issue a written warning (by email) to the Member, clearly describing the infringement and setting a deadline for corrective action.

If normal behaviour does not resume within the defined timeframe, exclusion from the CCFAI group may be considered in accordance with Articles 11.1 and 11.2 of the EUCC ISAC Statutes, depending on the seriousness and impact of the misconduct, and after giving that Member the opportunity to be heard in its defence.

Exclusion may be temporary (gradually: suspension for one (1) physical meeting or six months, then two (2) physical meetings or one year) or permanent, depending on the circumstances.

The Chairman shall present the case to the CCFAI during its next meeting and request a vote on the proposed exclusion. The decision shall be taken by simple majority, following the voting rules set out in Article 13 of these TOR.

10. Meetings

Face-to-face meetings are recommended and shall be held at least two (2) times per calendar year. Between physical meetings, CCFAI shall hold regular online meetings (typically at least one per month) and may organise ad-hoc working sessions on specific topics. Physical meetings are hosted by one of the group Members on a voluntary basis.

Each meeting shall commence with an overview of the agenda, approval of minutes from the previous meeting and a reminder of the EUCC ISAC Antitrust Compliance Guidelines. The following text may be used to meet this requirement:

> *Attendees are kindly reminded that the EUCC ISAC is committed to complying with all relevant antitrust and competition laws and, to that end, has adopted Antitrust Compliance Guidelines. Failure to abide by competition laws can have extremely serious consequences for the EUCC ISAC and its participants, including heavy fines and, in some jurisdictions, imprisonment for individuals. In particular, it is strictly prohibited to discuss commercially sensitive information such as prices, costs, customer details or production plans with competitors. This applies not just to formal meetings but also to informal discussions. You are therefore asked to familiarise yourself with the Antitrust Compliance Guidelines and to strictly abide by the rules at all times.*

The Chair may request the presence of external antitrust counsel at meetings expected to involve a discussion on a potentially sensitive issue. In the event that a topic being discussed is considered to raise sensitive issues in particular relating to competition law compliance, the Chair or the Vice-Chair has the right to suspend the discussion pending external legal advice on the subject. This suspension shall be recorded in the minutes of the meeting concerned.

11. Late Membership fee policy

The following policy applies where membership fees due by a Member have not been received by EUCC ISAC within the timeframe aforementioned:

a. After 60 days of the due date set in the invoice, the Secretariat sends a first reminder letter or email to the Member that the payment is now 60 days past due and notifies the Board.

b. 45 days after the first reminder letter or email (1) the Secretariat sends asecond letter or email that the membership rights and benefits will be temporarily suspended if payment is not received within 30 days and notifies the Board.

c. 30 days after the second reminder letter or email (2) the membership rights and benefits are suspended. According to the bylaws, the Board may waive (or delay) the suspension based on individual case.

The Secretariat may use the services of a recovery fee company to collect unpaid membership fees, subject to approval from the Board.

12. Voting rules

Prior to a vote being required, it should be communicated to the Members that a vote will take place. This may be achieved by including a statement in the previous minutes, or by notifying Members at least 2 weeks prior to the next meeting. A failure to comply with this formality means that the vote must be postponed to the next meeting unless all CCFAI ISAC Members first agree unanimously to proceed with the vote (for the avoidance of doubt, this means that all CCFAI ISAC Members eligible to vote must be present in person or remotely at the meeting).

Although it is encouraged that Members should attend all meetings it is noted that this is not always possible, it is therefore allowed for Members to register a vote by email prior to a meeting.

All votes are tallied, and the majority is taken into account. For a measure to pass the yes votes must be more than 50% of the votes cast unless otherwise stated in these Terms of Reference.

A vote is considered as one vote from one Member of CCFAI irrespective of the number of representatives (or subsidiaries) of the Member active in CCFAI. This means that if an organization has multiple Members, then they have only one shared voting right.

If the two conditions are not met, the vote should be postponed until the next meeting.

In order to validly deliberate and take decisions, at least more than one half of the Members must be present or represented. Subject to a quorum being present, a decision of CCFAI shall be taken by a simple majority of the votes.

A Member may give a power of attorney in order to be represented at a meeting of CCFAI ISAC. An attending Member cannot receive more than 2 Power of attorney.

13. Alteration to the Terms of Reference

In order to validate any alteration to the Terms of Reference, a quorum shall consist of at least fifty percent (50%) of the voting Members, either present or represented. Subject to a quorum being present, any decision shall be taken by a two-thirds (2/3) majority of the votes cast.

A Member may give a power of attorney in order to be represented at a meeting of CCFAI ISAC. An attending Member cannot receive more than two (2) Power of attorney.

Although it is encouraged that Members should attend all meetings it is noted that this is not always possible, it is therefore allowed for Members to register a vote by email prior to a meeting.

14. Output Materials

Documents generated by CCFAI are owned by the EUCC ISAC and are made available to the members or public for non-commercial purposes.

Documents generated by the subgroups of CCFAI shall be returned to the main group for final approval.

It should be noted that the host of the Output Material may require to review and send comments back to CCFAI as part of its release process. Any substantive amendments must be approved by the CCFAI Members by majority vote prior to resending it for final validation. The CCFAI Chair shall then communicate the Output Material to the external party for publication.

The members can use information discussed in the meetings or communicated in the documents in their respective organization.

Nothing in this document shall cause prejudice to national laws and regulations of the Member States, including regarding public access to documents, government access to documents, the protection of personal data or the protection of classified information.

15. Chairman of CCFAI

The Chairman oversees steering meetings and sub-group activities. The Chairman is responsible for chairing meetings and ensuring minutes of each meeting are recorded and distributed. The Chairman proposes the agenda for each meeting.

The mandate of CCFAI Chair and Vice-Chair is from 1st January to 31st December per calendar year.

The Chair is accountable to gather and achieve the CCFAI group objectives. These objectives can be self-assigned, or assigned to CCFAI by ISAC steering Committee, ECCG (EsEm). The Chair is also accountable for CCFAI outputs (in terms of operations/timing, not in terms of technical content[1]), CCFAI way of working (checking Member participation, creation of subgroup, moderation of CCFAI plenary meeting, the respect of Terms of References ...) and any external communication with all stakeholders (ISAC steering, ECCG (EsEm), Eurosmart...).

The Vice-Chair is the Chair deputy, assisting the Chair in all meetings and its tasks, in particular the consolidation and review of CCFAI outputs.

The Chairman and the Vice-Chair seat at the steering committee of the EUCC.

The election of the CCFAI Chair and Vice-Chair should take place once a year, normally during the last meeting per calendar year. Candidates should inform the Chair and the Members of their interest to become Chair or Vice-Chair at least two weeks prior to the proposed election. If there are no proposed new candidates, then the current Chair and/or Vice-Chair may continue in the role without a formal vote being required. The Chair and the Vice-Chair seats at the steering committee of the EUCC ISAC.

Members may bring any serious concerns relating to the conduct of the Chair or Vice-Chair to the attention of the CCFAI Members and ask for an extraordinary vote, voting will then take place to agree to replace the Chair by a 75% majority. An election is then held at the next full meeting.

16. Sub-groups of CCFAI

Sub-groups can be created to work on specific topics which cannot be managed during ordinary meetings of CCFAI. Sub-groups are subjected to prior validation of the Group members pursuant to article 8 and shall be validated by the steering committee of the EUCC ISCA. The competence of the sub-

[1] technical content accountability is conferred by the expertise of the Members.

group shall be limited to the scope of CCFAI to avoid any prejudice to the work of the other EUCC ISAC technical groups.

CCFAI defined the subgroups' roadmap, subgroups report to CCFAI at least every 3 months. Due to workloads and precision of some tasks, CCFAI may wish to establish one or more Sub-Group(s) to focus on issue concerned.

Any Member can propose the establishment of a Sub-Group and Tasks. The Members will vote on the establishment by majority vote. The vote follows the rules defined in Article 12.

The Chair will propose a Sub-Group leader. The Members will then vote to accept or propose another candidate following the rules in Article 12.

The Sub-Group must follow the Terms of Reference and is answerable at all times to the CCFAI Chair and Vice-Chair.

It is the responsibility of the Sub-Group leader to organize meetings and prepare or delegate the minutes for the Sub-Group. The Sub-Group leader must also report back to CCFAI when required by the CCFAI Chair or Vice-Chair.

Reporting includes:

- Timelines
- Output
- Meeting reports
- Status reports

The Sub-Group leader is entrusted to chair sub-group meetings and ensure that rules for Members are adhered to. If a sub-group requires to change the leader, then they may vote to replace the chair.

The proposal is then made to the main group by email. If no objections are made within a 2-week period, then the new sub-group leader is appointed. Any objections would then trigger a vote following the rules defined in Article 12.

A chairman oversees the work of the sub-group. They shall be appointed by CCFAI pursuant to article 8 for a limited period of one year. Their mandate could be renewed.

17. Intellectual Property Rights (IPR) Policy

CCFAI's activities are conducted in strict compliance to the IPR policy of the EUCC ISAC. (Annex A).

Each Member shall use its reasonable endeavour's to timely inform CCFAI of that Member's Essential IPR that the Member is aware of and believes to be likely to fully or partially cover elements of Specifications that are being developed by a Member of CCFAI prior to such Specifications being submitted to a voting procedure. In particular, each Member submitting a technical proposal for development of a Specification shall timely and on a bona fide basis draw the attention of CCFAI to the IPR of that Member which might be Essential if the proposal is adopted.

18. Antitrust Compliance

The EUCC ISAC and CCFAI's activities are conducted in strict compliance with applicable antitrust laws. CCFAI's Members shall respect the Antitrust Compliance Guidelines (Annex B)..

The CCFAI activities must not lead towards a restriction of competition between Members, nor must meetings of Members organized or supported by CCFAI be used by Members to discuss or coordinate

market behaviour resulting in a restriction of competition. More generally, the platform offered by CCFAI to its Members must not be misused for activities prohibited by antitrust laws.

A reminder of general rules including antitrust will be done at each meeting start and in the minutes of meeting.

19. Anti-Corruption and Influence Peddling

The Members of the EU CC ISAC and CCFAI shall always act in compliance with the applicable national and international laws and regulations governing the detection and prevention of corruption and influence peddling risks.

Neither Party, whether directly or through third parties, shall offer to, nor accept from, any person an offer, promise, gift, present, or any advantage that could be linked to an abuse by that person, committed or potentially committed, of their real or perceived influence, with the aim of obtaining for themselves or others a distinction, employment, contract, or any other favourable decision.

Neither Party shall solicit or accept for themselves any offer, promise, gift, present, or any advantage in exchange for abusing their influence to make or obtain any favourable decision.

20. Data Processing and Data protection

Members of CCFAI may process personal data for the purposes of administrative management and the exchange of information related to the execution of the activities conducted by the EUCC ISAC.

The Members of CCFAI respectively determine the purpose and means of the aforementioned processing, each acting as a data controller.

The Members of the Association undertake to comply with the regulations on personal data protection applicable to the agreement, including Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (GDPR).

The Members of the Association agree to process only the personal data strictly necessary for the execution of the activities conducted by the EUCC ISAC.

The personal data processed by the Members of the Association include the contact details of other Members and/or any third parties, such as their name, first name, professional identifier, role, professional email address, workplace, and phone number.

The Members of the Association commit to informing the aforementioned data subjects of the processing of their personal data.

21. Confidentiality and Information Protection

Members of CCFAI acknowledge that participation in its activities may involve access to confidential information.

Members of CCFAI acknowledge that participation to its activities may involve access to confidential information. Members shall agree to treat all such information with the same degree of care as they would their own confidential information, but in any case, no less than reasonable care. Confidential information shall not be disclosed to any third party except as expressly permitted by the CCFAI confidentiality provisions.

Members shall ensure that their representatives respect these confidentiality obligations. Information shared within CCFAI shall be presumed non-confidential unless designated otherwise in writing and accepted as such by the Chair.

Any confidential information disclosed remains the property of the disclosing party and must not be copied, used, or disseminated beyond the agreed scope.

These obligations shall survive the termination of a Member's participation for a period of 15 years from the date of disclosure, unless explicitly released in writing by the disclosing party.

22. Complaint Procedure

This section details procedures for complaints and appeals that concern the actions and decisions of CCFAI and its Subgroups related to the release of a specification, a technical document or a publication.

Conditions

Complaints may only be submitted by persons or organizations that are directly, materially, or adversely affected by the activities related to the complaint.

Complaints filed with the EUCC ISAC must:

- be introduced within 30 days after the EUCC ISAC has officially communicated a specification or a technical document or a publication;
- be accompanied by documentation providing all relevant details of the complaint;
- include any supporting evidence or documentation, such as statements and explanations related to the issue; and
- not be repeated unless a minimum of 6 weeks has passed.
- pay attention on that the complainant (person or organization) shall not derive any rights or presume the validity of the claim based on the fact that the EUCC ISAC is investigating the complaint.

Process

The complaint shall be submitted by e-mail sent to the Secretariat at contact@ccisac.eu

The complaint, along with the personal and/or company information of the complainant (full name, address, and other contact details), shall include the complainant's personal opinion about the assessment and/or conclusion, the reasons for disapproval with the decision reached, as well as the settlement being sought.

The Secretariat will acknowledge receipt of the complaint, assign a complaint reference number (CPYYYYMMnn), the Board appoints the person responsible for investigating and assessing the complaint, The selection is based upon competence, independence and impartiality. Then, the Secretariat notifies the person of the complaint.

The person responsible will investigate and assess the complaint, considering advice from the technical experts, where necessary, to determine the facts of the case and an appropriate response or resolution.

This investigation will be completed within 30 days of receipt of the complaint. If more time is needed, the complainant will be notified of progress and estimated timeline.

Proposed resolutions will be reviewed and ratified by the Steering Committee for determining a final decision prior to onward communication.

The Secretariat will communicate outcomes or proposed resolutions to the complainant.

If the complainant agrees with the outcome at this stage, then the complaint does not proceed to further stages and the complaint is closed.

If the complainant is not satisfied with the outcome, then they may submit an Appeal.

Records of complaints, investigations, and proposed resolutions will be provided to and maintained by the Secretariat.

23. Appeal Procedure

This procedure stipulates the way in which an appellant may appeal a decision of the EUCC ISAC with respect to a complaint.

Filing

Appeals may only be submitted by persons or organizations that are directly, materially, or adversely affected by the activities related to the initial complaint / appeal.

The appeal must be submitted within 14 days after the decision on the disputed complaint is communicated to the complainant.

The appeal shall be submitted by e-mail sent to CCFAI Chair and Vice-Chair email.

Acceptance

The appellant can only submit an appeal after the Secretariat has communicated a final decision on the complaint.

If the appeal is submitted within the required timeline and by the appropriate person or organization and no prior appeal has been submitted, the appeal will be accepted by the EUCC ISAC, with no undue burden imposed on the appellant.

When an appeal has been accepted by the EUCC ISAC, the appeal is considered formal and will be dealt with according to this procedure.

Process

Upon acceptance of an appeal, the Chair will promptly acknowledge receipt and assign an appeal reference number (APYYYYMMnn). The Steering Committee selects the person responsible for investigating and assessing the appeal. The selection is based upon competence and independence/impartiality.

The person responsible for investigating and assessing appeals will be notified of the filed appeal.

The person responsible will investigate and assess the appeal, taking into account advice from the technical experts where necessary, to determine the facts of the case and an appropriate response or resolution. This investigation will be completed within 30 days of receipt of the appeal. If more time is needed, the appellant will be notified of progress and estimated timeline.

All appeals will be handled by the relevant parties promptly and in a fair, unbiased, and impartial manner.

Proposed resolutions will be reviewed and decided expeditiously by the Steering Committee prior to onward communication.

The Secretariat will communicate outcomes of the final decision to the appellant and the appeal is closed. Note that appeals may not be repeated or re-submitted.

Records of appeals, investigations, and proposed resolutions will be provided to and maintained by the Secretariat.

24. Annexes

Annex A: IPR Policy of the EUCC ISAC – https://ccisac.eu/wp-content/uploads/2025/07/2024_11_25_EU-CC-ISAC-IPR-policy.pdf

Annex B: Antitrust guidelines - https://ccisac.eu/wp-content/uploads/2025/09/EUCCISAC_Antitrust-Compliance-Guidelines_.pdf

Reference:

- EUCCISAC Articles of Association EUCC ISAC AISBL V1.0 – 15 January 2025 https://ccisac.eu/wp-content/uploads/2025/07/EUCCISAC_articles-of-association.pdf

About us

The EU Common Criteria Information Sharing and Analysis Centre (EUCC ISAC) is an international non-profit association dedicated to fostering collaboration, harmonization, and excellence in cybersecurity certification.

The EUCC ISAC acts as a central hub for collaboration between public and private stakeholders, ensuring the effective and consistent implementation of the EU Common Criteria (EUCC) certification scheme. It provides essential input to key entities—including the ECCG subgroup for EUCC maintenance (EsEm), the European Commission, ENISA, and Member States—to support the ongoing development and maintenance of the EUCC scheme. We aim to maintain state-of-the-art practices by providing technical interpretations, methodologies, attack quotations, and an up-to-date attack catalogue.

EUCC ISAC | Avenue de Broqueville, 66 - 1200 Brussels – Belgium | contact@ccisac.eu

EUCC ISAC