

# ISO/IEC 15408 Standards: Some Key Stakeholders



## Other Stakeholders

Different verticals,

Eg

- Healthcare
- Finance
- Dependability
- High Assurance
- Automotive
- Embedded Devices
- Academic

Technology focused technical communities, eg smartcards, biometrics, NIAP PPs, CCRA supported iTCs etc,

**May** be associated with specific schemes or MRA, ISO/IEC 15408 certification and recognition  
E.g. Global Platform, Open Group

## Other MRA and Schemes

E.g. SOG-IS, CNITSEC (China), Russia

Typically related to Govt. Agency use/ National / Regional regulation

Use the criteria in accordance with their own policies. / Arrangements

Often produce supporting documents, PPs etc.  
May be technology specific eg Smartcards

## ISO/IEC JTC 1/SC 27 WG3

Open to all ISO members and Liaison organizations

- 52 Participating nations
- 21 Observing nations
- 42 Liaison orgs

Scope includes “Common Criteria” for all stakeholders.

Produce other IA standards, eg crypto modules, biometrics, guidance.  
Guidance and docs related to 15408

MRA and Scheme policies are out of scope

## CCRA: CCDB

Open to CCRA signatories

- 17 authorizing
- 10 consuming

Scope is “Common Criteria” standards and supporting documents as needed by CCRA membership (National Agencies only).

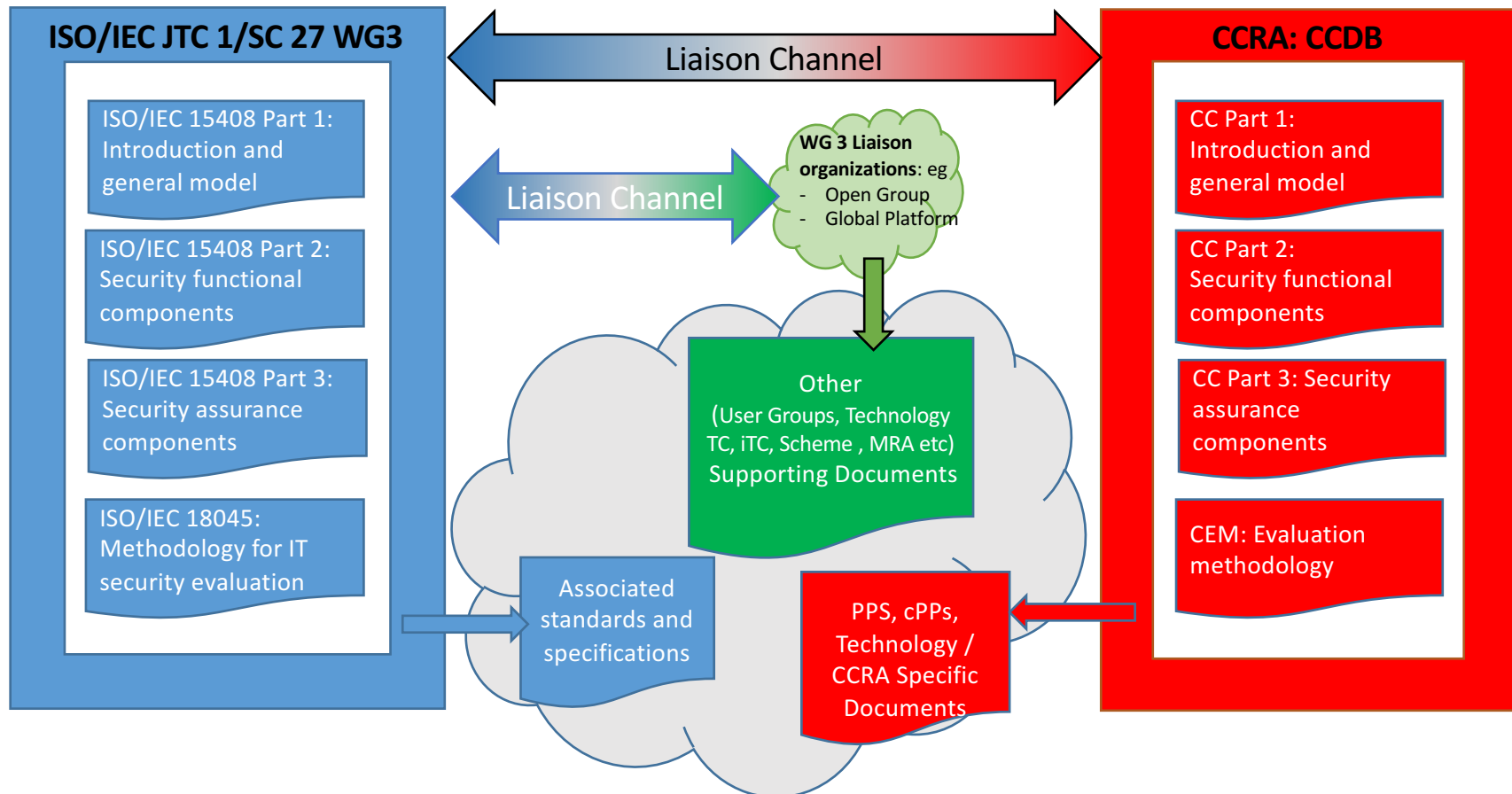
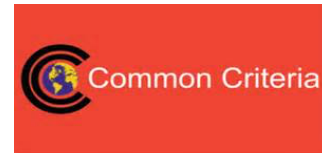
CCRA and Scheme policies are in scope. Other MRA and use-cases are not within the scope of the CCRA.

Fosters iTCs and “sponsors cPPs”

A major user of the CC



## How the Common Criteria Standards are Developed Today



# SC 27 WG 3 Mission

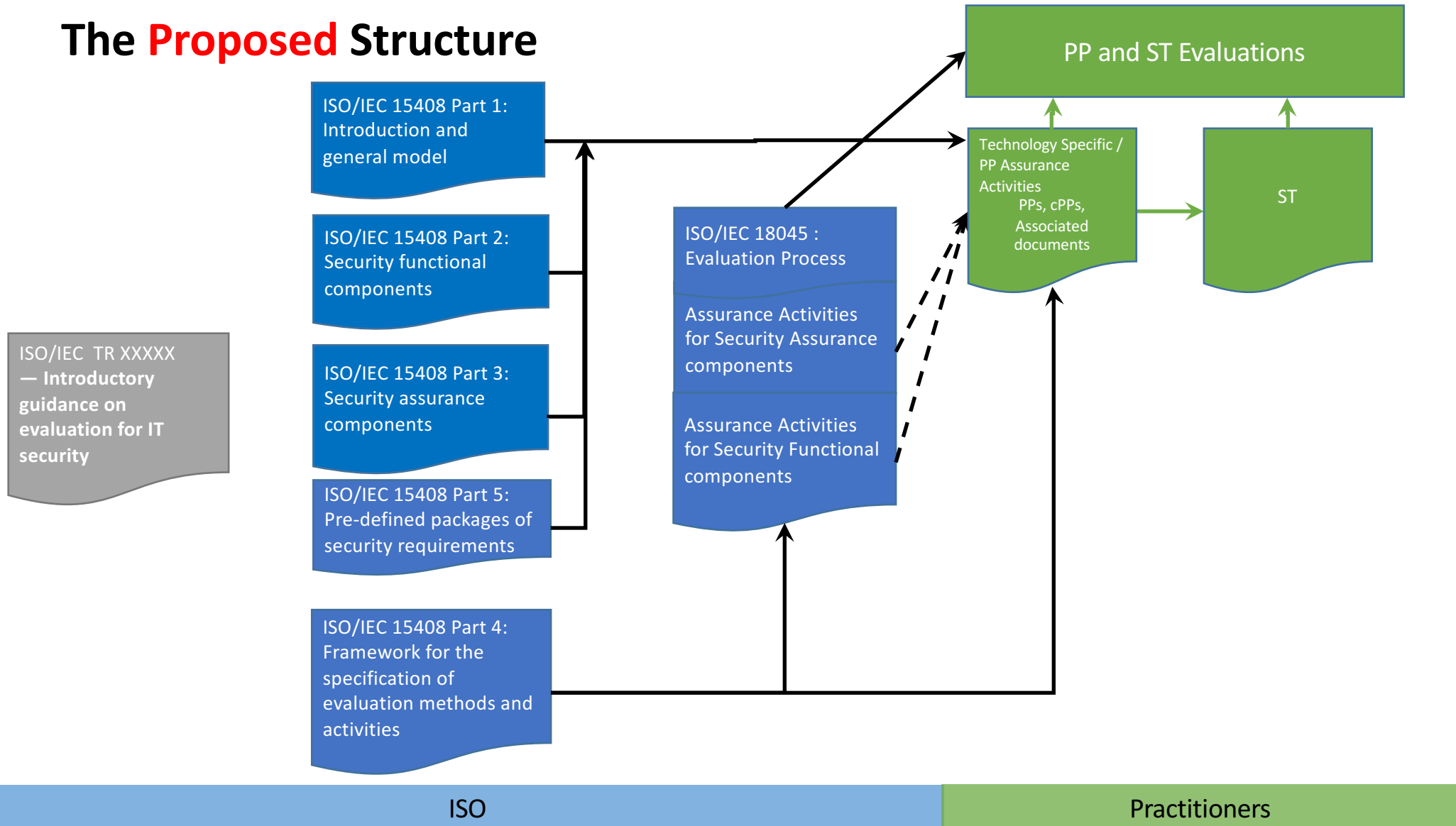


## Security Evaluation, Testing and Specification






The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:





- a) security evaluation criteria;*
- b) methodology for application of the criteria;*
- c) security functional and assurance specification of IT systems, components and products;*
- d) testing methodology for determination of security functional and assurance conformance;*
- e) administrative procedures for testing, evaluation, certification, and accreditation schemes.*

# The Proposed Structure

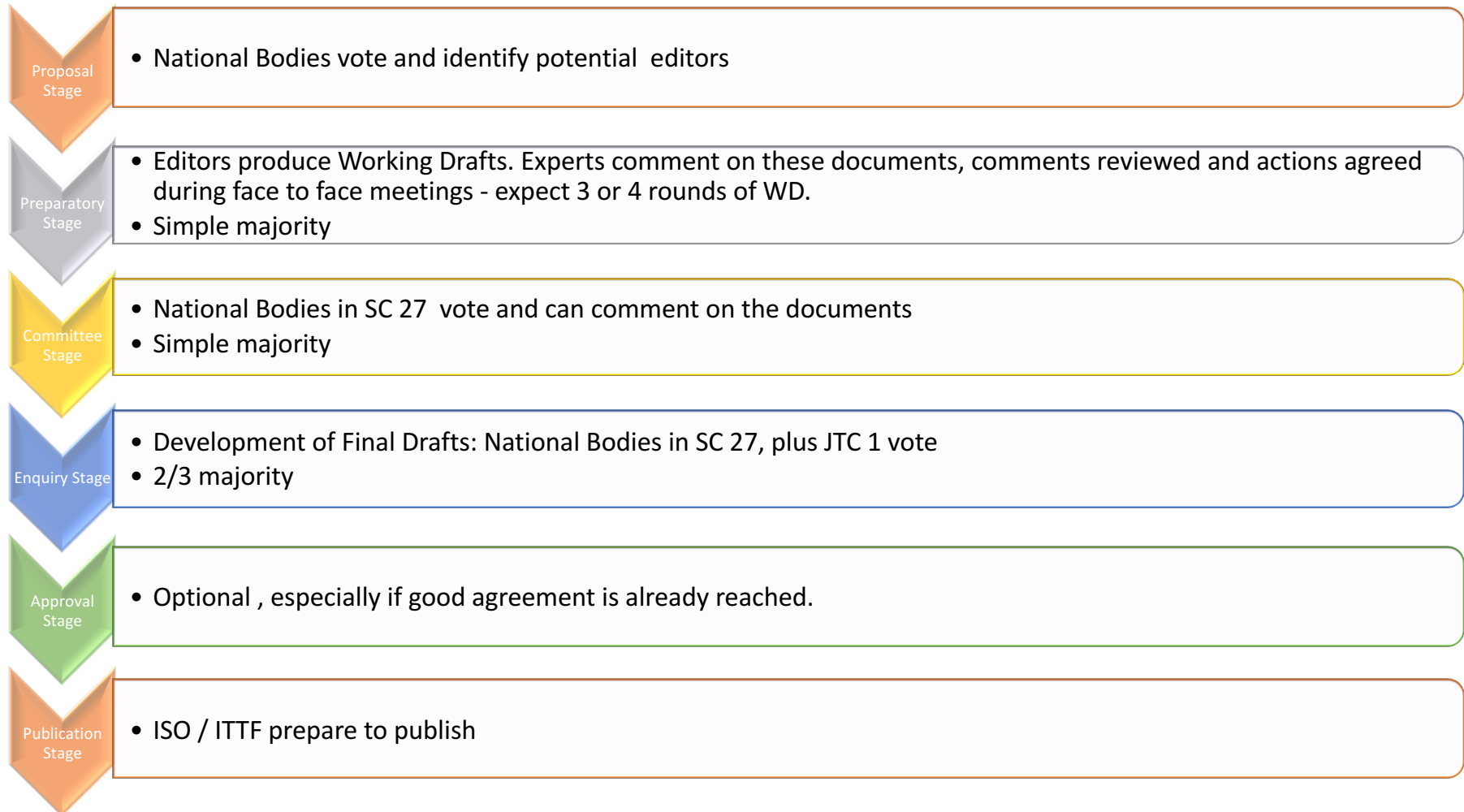


# Expected Content (High-level)

- ISO/IEC 15408 Part 1: Introduction and general model**  Revise to
  - allow the model of CCDB's vision
  - Include basic modularization
  - Review definitions
  - Exact Compliance
  - Address changes derived from contributions to SP, and other sources
- ISO/IEC 15408 Part 2: Security functional components**  Revise to
  - Include SFRs in common use but not defined
  - Review and update SFRs
- ISO/IEC 15408 Part 3: Security assurance components**  Revise to
  - Move EAL & CAP to part 5
  - Address changes agreed to from contributions to SP, and other sources
- ISO/IEC 15408 Part 4: Framework for the specification of evaluation methods and activities**  A standard framework for writing GOOD Assurance Activities
- ISO/IEC 15408 Part 5: Pre-defined packages of security requirements**  The set of pre-defined packages that the standard offers to the world. (eg EALs, CAPs from current part 3), but will also be used to support eg SFR packages supporting modularization etc.

- ISO/IEC 18045: Evaluation Process**  The evaluation process for Labs Contains the basic evaluation process. Cf 18045(CEM) Section 7. But with major review
- Assurance Activities for Security Functional components**  The core assurance activities for SFRs
- Assurance Activities for Security Assurance components**  The core assurance activities for SARs
- ISO/IEC TR XXXXX — Introductory guidance on evaluation for IT security**  A technical report giving transition guidance and other information relating to the changes.

## Key Points of the Development Process in ISO/IEC JTC 1



This presentation is simplified: See the ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2016 for the full rules

## So what happened to my contributions to the Study Period?



- These were initially used at a high-level by WG 3 to determine if we needed to review the structure of the standards, need new items etc.
- If the proposal for the structure change is approved by the NBs, and once editors are assigned, contributions will be reviewed by the editors in more detail in order to produce the first working drafts.
- Contributors will be expected to actively participate in this phase to ensure that the editors understand and integrate contributions in a satisfactory manner.
- The proposed new TR is also intended to cross reference the inputs from study period.
- Items that are not mature, or where good agreement in the WG cannot be found, will be placed on the WG 3 Roadmap so the WG can manage them appropriately.

# Potential WG3 Roadmap Items

**Composition (detailed)**

**Use of Registration Authorities**

**Vulnerability Analysis**

**Assurance maintenance**

**Site certification – reuse site certification assurance in a product eval.**

**ISO/IEC 15543 (FRITSA)**

- General IA framework description?
- Metrics?