Moving Forward with ISO

Changes in the 2020 revision of ISO/IEC 15408

- Restructuring and updating the standard and concepts
- Specification based approach

- Efficiency in Evaluations
- Technology evolution: New and changed SFRs

Restructuring the Standard

- How to write evaluation methods/activities (Part 4)
- Move packages (e.g. EAL) into Part 5
- An ontology for 15408 concepts
- Concepts of Composition explained

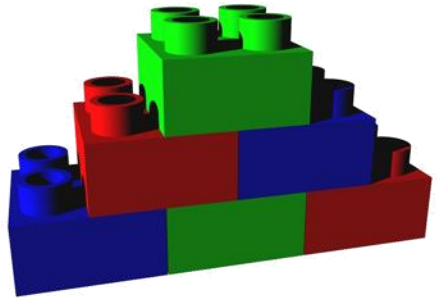
Exact Conformance

- Was introduced in the CC-Addenda for CC 3.1 R5.
- Has been under trial (especially with U.S. NIAP).
- Can be used with modularization.
- Is appropriate to use in a specification based approach for security requirements.

Specification based approach

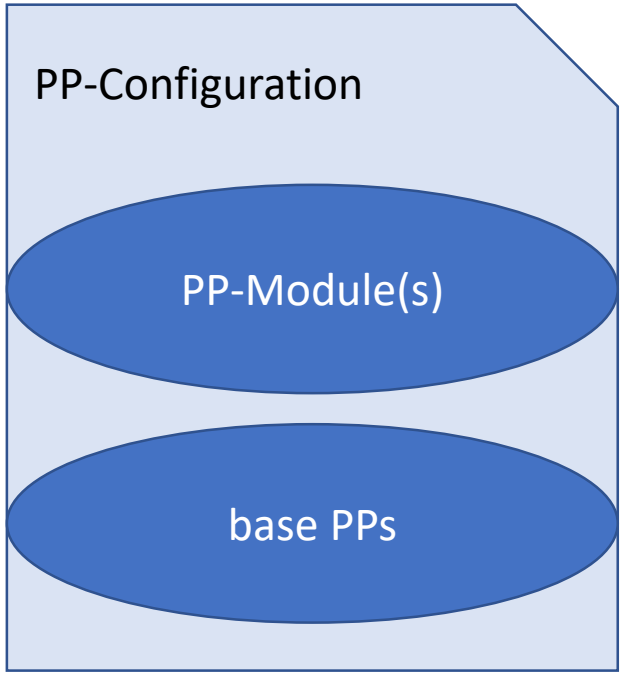
Attack based approach

Efficiency: Modularization

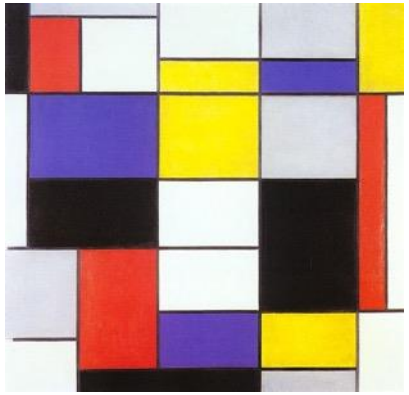


- Was already introduced in CC 3.1 R5, but is refined in the ISO draft
- Allows to construct (“virtual”) PPs using a modular approach
- Allows to define SFR/SAR packages within PPs and PP-Modules
- Can be used with
  - Multi-Assurance
  - all kinds of conformance (Exact, Strict and Demonstrable.)
  - Direct Rationale

(Although mixing these is not always allowed!)



Efficiency: Multi-assurance

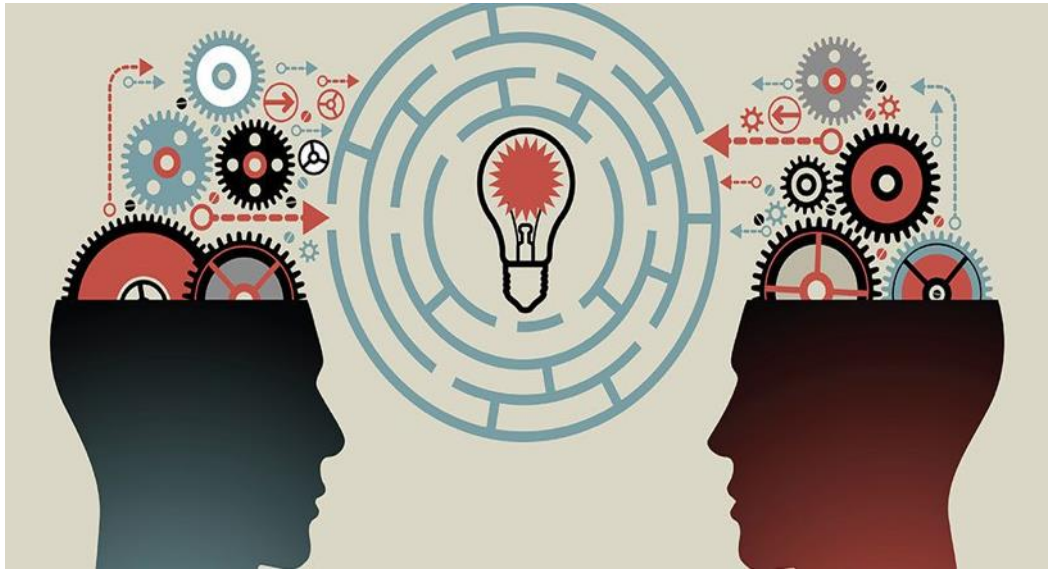


- Extends the notion of evaluation to products that consists of heterogenous functions/components which deal with assets of different sensitivity
- Allows to define assurance packages at PP-Module level
- Allows to combine multiple assurance packages in one PP-Configuration, coming from the base PPs and/or PP-Modules
- Allows to define a global assurance package at PP-Configuration level that applies to the entire TOE
- The assurance packages can be predefined EALs or any well-formed standard or extended SAR package
- Origin: Concept introduced in the framework of payment terminals (POI PP), generalized in the revision of the standard

Efficiency: Direct Rationale

- Intended for less complex PPs and STs
- Allows to map the SFRs and the security objectives for the environment directly to the SPD
- Requires natural language descriptions of SFRs
- Low-assurance PPs and STs (as found in CC 3.1 R5) are no longer allowed by the 15408 standard

What are the new SFRs?



- **FCS_RBG** (Random bit generation)
- **FCS_RNG** (Generation of random numbers)
- **FIA_API** (Authentication proof of identity)
- **FMT_LIM** (Limited capabilities and availability)
- **FPT_EMS** (TOE emanation)
- **FPT_INI** (TSF initialization)
- **FTP_PRO** (Secure channel)

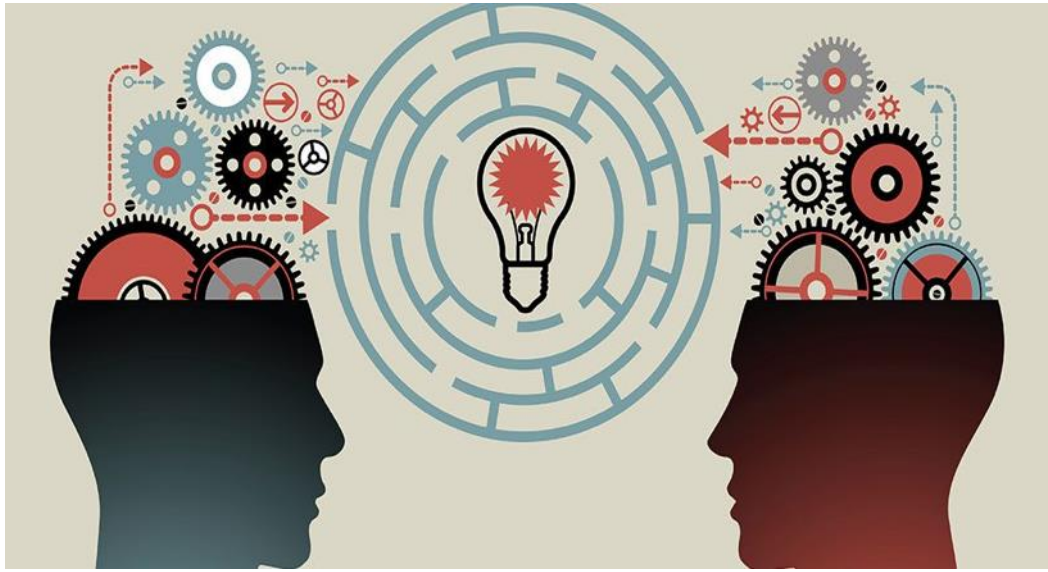
CD2 will include a call for contribution for some of the SFRs

Which SFRs have changed?

- **FCS_CKM:** Cryptographic key management (New components and re-leveled)
- **FDP_SDC:** Stored data confidentiality (Modified to better incorporate notions such as full disk encryption)
- **FIA_UAU:** User authentication (Dependencies changed)
- **FPT_STM:** Time stamps (Added component)
- **FTA_TAB:** TOE access banners (Includes selections and assignments)
- **FPR_UNL:** Unlinkability (Includes new components)

Some SFRs are under definition within CCDB

What's about the SARs?



- **10 New SAR (compared with CC V3.1 R5)**
  - **xxx_COMP.1 [ASE, ADV, ALC, ATE, AVA]:** composite evaluation
  - **ALC_PTD.1,2,3:** Practices for trustable development (will become ALC_TDA, TOE Development Artifact)
  - **ACE_OBJ.2, ACE_REQ.2**
- **Many changed SARs**

Jaipur
Tampa
Abu Dhabi
Hamilton
Berlin
Wuhan
Gj0vik
(Tel Aviv)

The Revision Journey

The plan for ISO/IEC 15408 & ISO/IEC 18045

Working drafts (2)	**2017**	**On time**
Committee drafts (2)	**2018**	**On time**
Draft International Standard	**2019**	
Publish	**2020**	

Representation in WG3 at Gjøvik meeting

National Bodies
Argentina
Australia
Canada
China
France
Denmark
Finland
Germany
India
Japan
Korea
Luxembourg
Malaysia
Mexico
Norway
Poland
Russia
Singapore
Spain
Sweden
UK
US

- 22 national bodies represented in the registrations to attend in Gjøvik *
- 105 people registered to attend WG3 in Gjøvik, with Good representation from schemes, developers, labs, and consultants/academics
- New liaisons established with the **CCUF** and SAFECode
- Good representation across technologies (smartcards, printers, ICs, OS, mobile, network, databases, biometrics, crypto modules, etc.)

Liaisons:
CCDB
CCUF
Global Platform
ISACA
ISO/IEC JTC1/ SC7 and SC37
ITU-T
SAFECode

**At Committee Draft, 52 participating and 25 observing nations will receive the documents and have the opportunity to comment on the documents*

Timetable for the next ISO drafts

The editors will produce the next drafts by: 2018-12-21

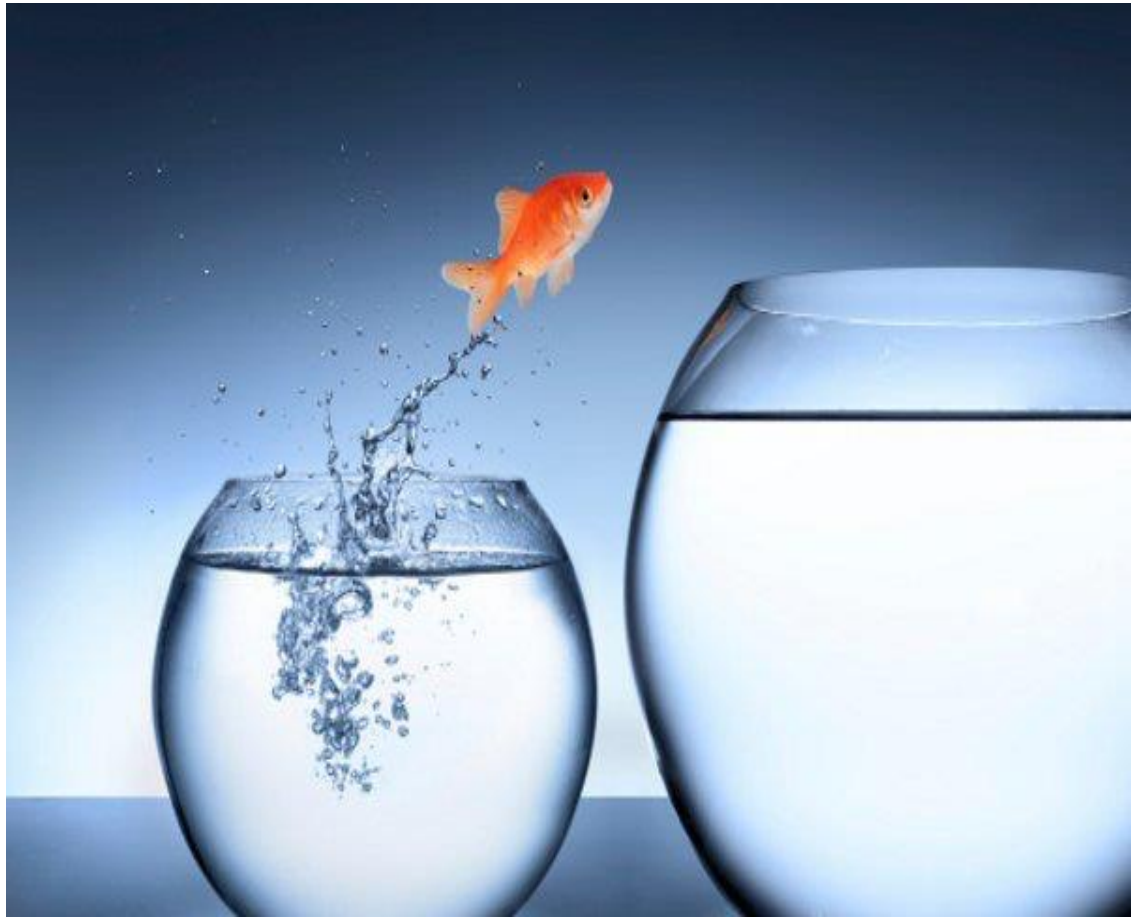
SC 27 will initiate the ballot on the CD2; comments (and NB vote*) will be required within 8 weeks: 2019-02-28

The editors will collate and review the comments and organize editing session(s) in the two weeks before the next WG 3 meeting in Tel-Aviv (April 2019).

** Note: Liaisons may comment but do not vote on the documents progression*

Transition – What should I be doing now?

- Review and comment on the CD2 draft
- Think about
  - Any necessary CCRA or other MRA changes
  - Needed Scheme changes
  - Developer strategies
  - Training/ education on the new standards
  - Updating PPs, cPPs etc..



How to contribute

- Via your National Body or
- Via a liaison organization (e.g. CCUF /CCDB)
  - To contribute via the CCUF please join the project “ISO standards” on Only Office at: https://ccusersforum.onlyoffice.com/products/projects/projects.aspx?prjID=534176

Good comments are

- Constructive,
- Provide suggested text, where appropriate,
- Do not conflict with or duplicate other comments from the same organization.