INTERNET OF TRUST

Transition to ISO/IEC 15408 & ISO/IEC 18045 New Concepts and Changes

Carolina Lavatelli (Internet of Trust)

Co-authors: Guillaume Tétu (ANSSI), Oana Andreescu (Internet of Trust)

19th October 2021

ICCC 2021

Abstract

The fourth edition of the ISO/IEC 15408 and ISO/IEC 18045 standards includes substantial changes. It allows to cover complex products and communities' needs and, at the same time, ensures compatibility with currently existing practices and processes.

The focus of this presentation is the Transition Guide that was developed all along the edition of the standards and whose aim is to help users understand the new concepts and related evaluation approaches, and switch from CC and CEM version 3.1 to the fourth edition smoothly.

Agenda

I. Introduction

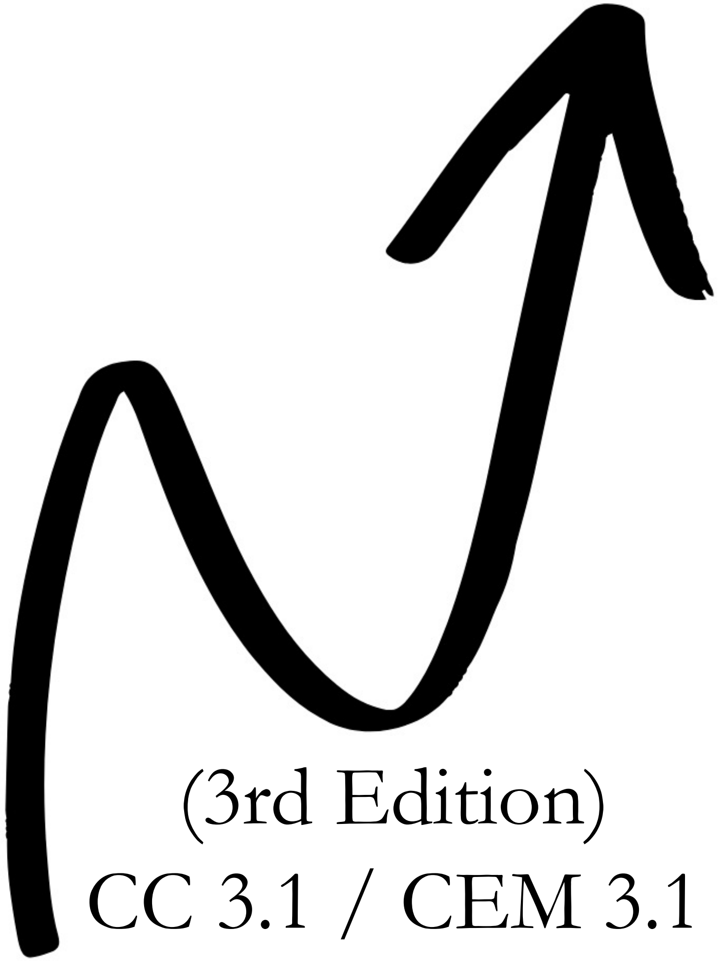
- ISO/IEC 15408 & ISO/IEC 18045 Revision in a Nutshell

II. Transition Guide – TR 22216

- Audience and motivation
- New structure of the fourth edition
- Content overview - changes and additions
- Documents navigation

III. Conclusion

ISO/IEC 15408 & ISO/IEC 18045 Revision - Objectives



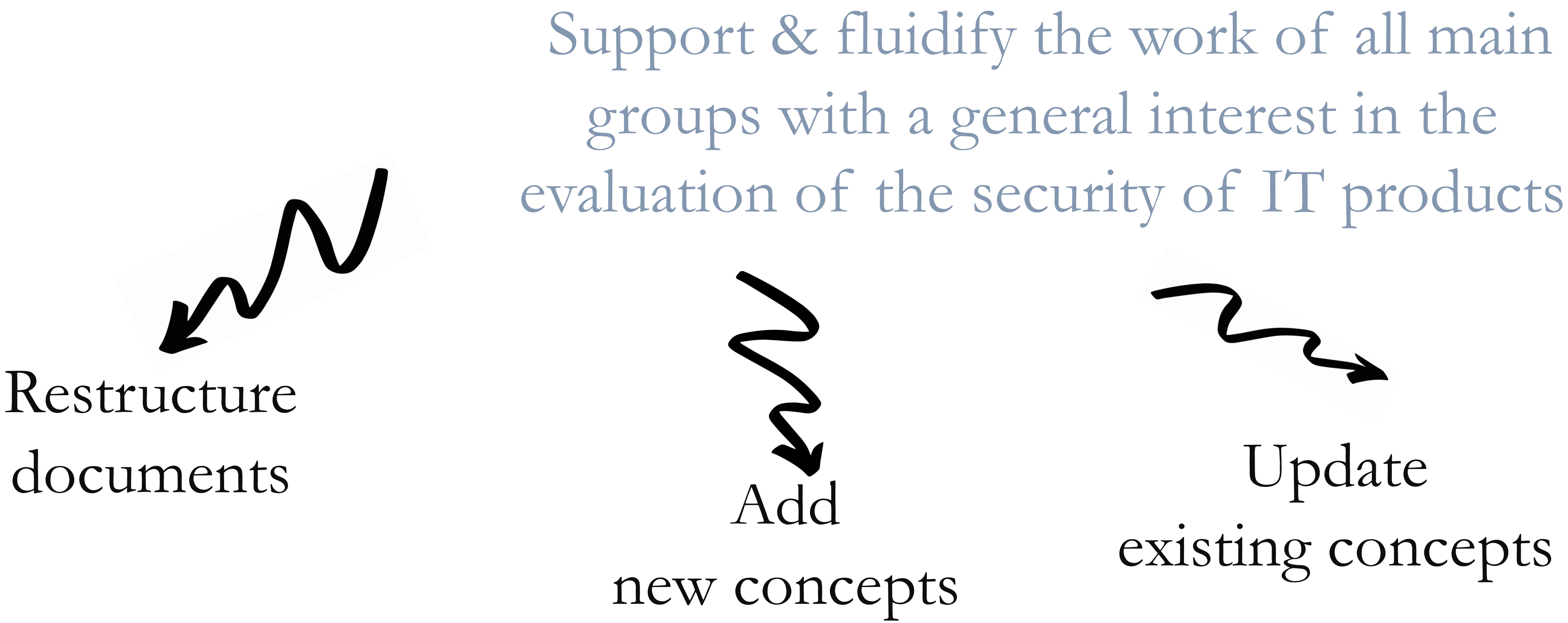
(3rd Edition)
CC 3.1 / CEM 3.1

4th Edition

Support & fluidify the work of all main groups with a general interest in the evaluation of the security of IT products

ISO/IEC 15408 & ISO/IEC 18045 Revision - Objectives

4th Edition



Support & fluidify the work of all main groups with a general interest in the evaluation of the security of IT products

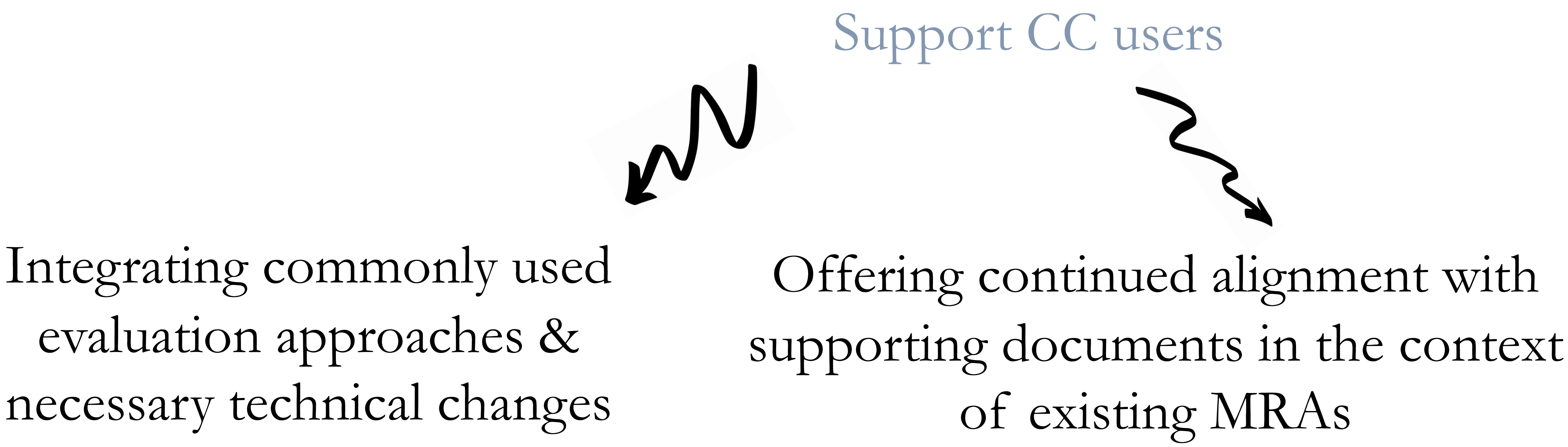
Restructure documents

Add new concepts

Update existing concepts

ISO/IEC 15408 & ISO/IEC 18045 Revision - Objectives

4th Edition



Support CC users

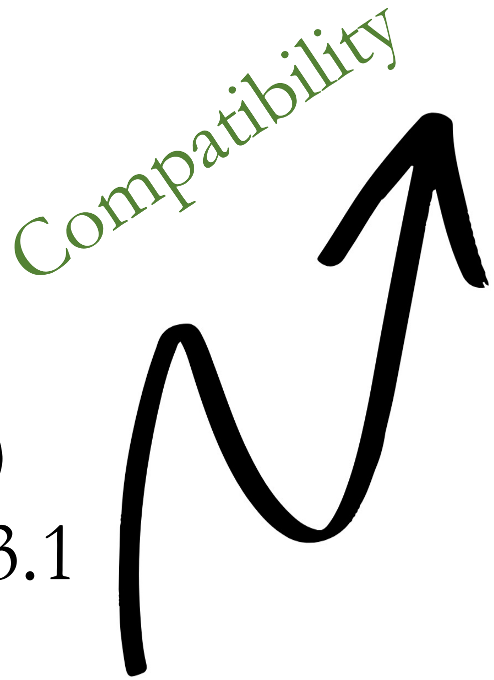
Integrating commonly used evaluation approaches & necessary technical changes

Offering continued alignment with supporting documents in the context of existing MRAs

ISO/IEC 15408 & ISO/IEC 18045 Revision - Effects

(3rd Edition)
CC 3.1 / CEM 3.1

Currently existing
practices &
processes



Compatibility

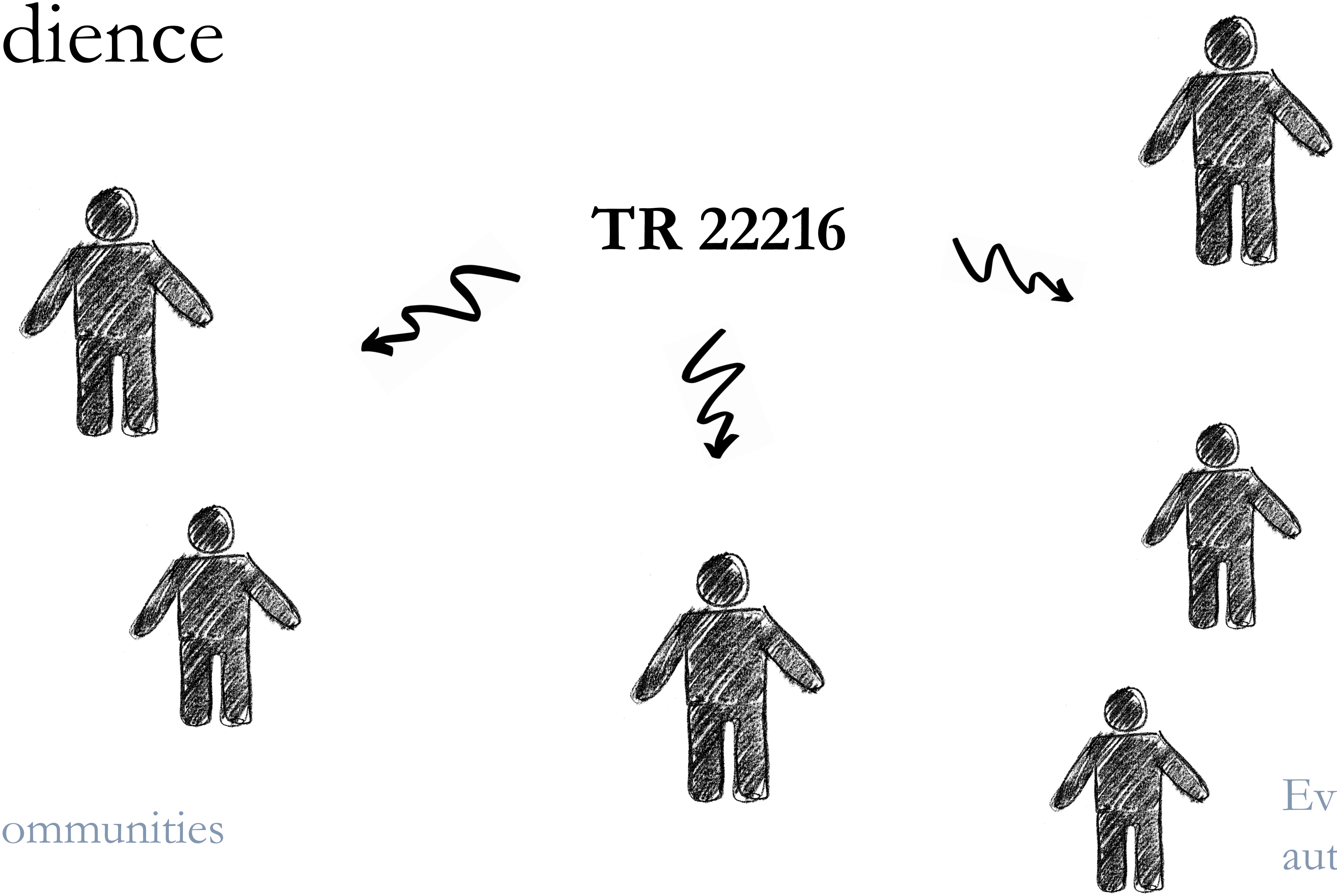
4th Edition

+ Expands the security specification & evaluation methodology toolbox

+ Is suitable for the definition of specific evaluation approaches

II. Transition Guide – TR 22216

Audience



TR 22216

Risk owners

Developers

Evaluators

Technical communities

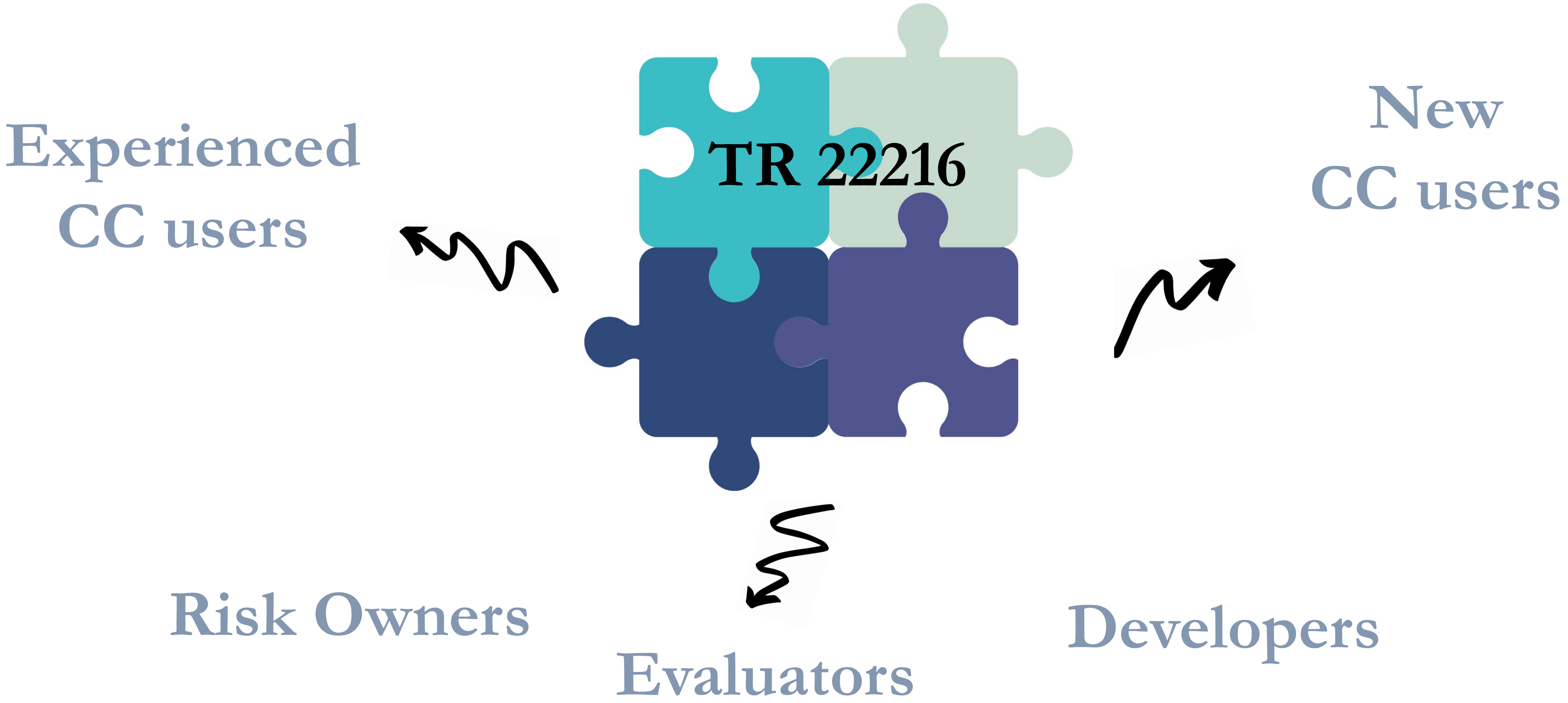
Consultants

Evaluation authorities

Motivation

For each concerned party, propose an evolution path & practical information for the transition to the 4th edition

Motivation



TR 22216

Experienced CC users

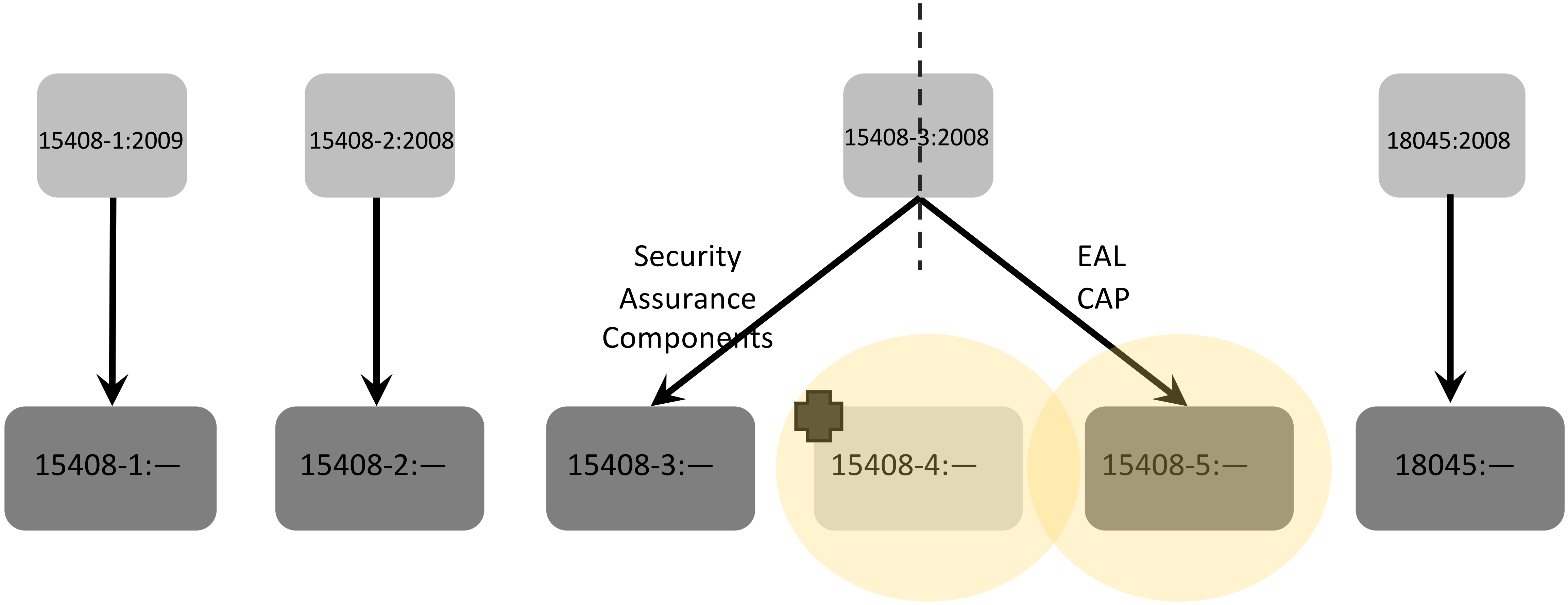
New CC users

Risk Owners

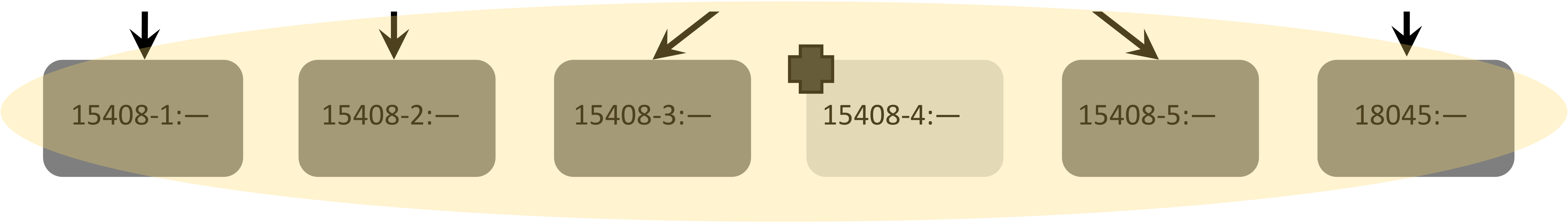
Evaluators

Developers

New structure of the 4th edition



Content Overview

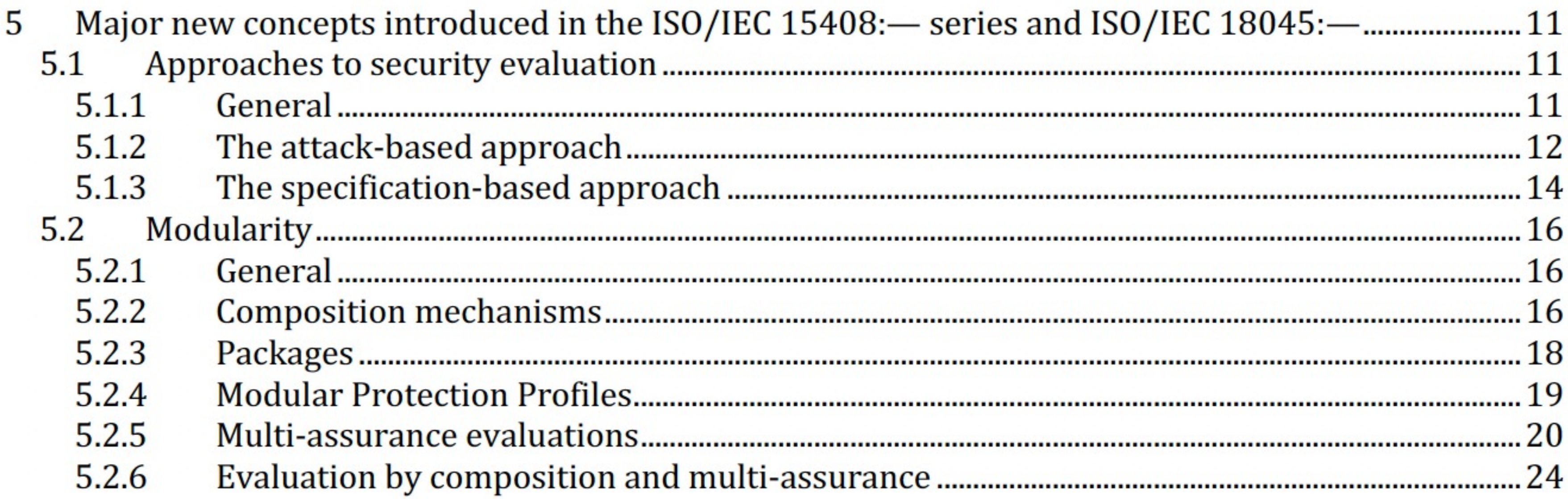


TR 22216 Clause 4

Presents the set of documents and briefly discusses the newly introduced concepts by parts and their impact on other parts.

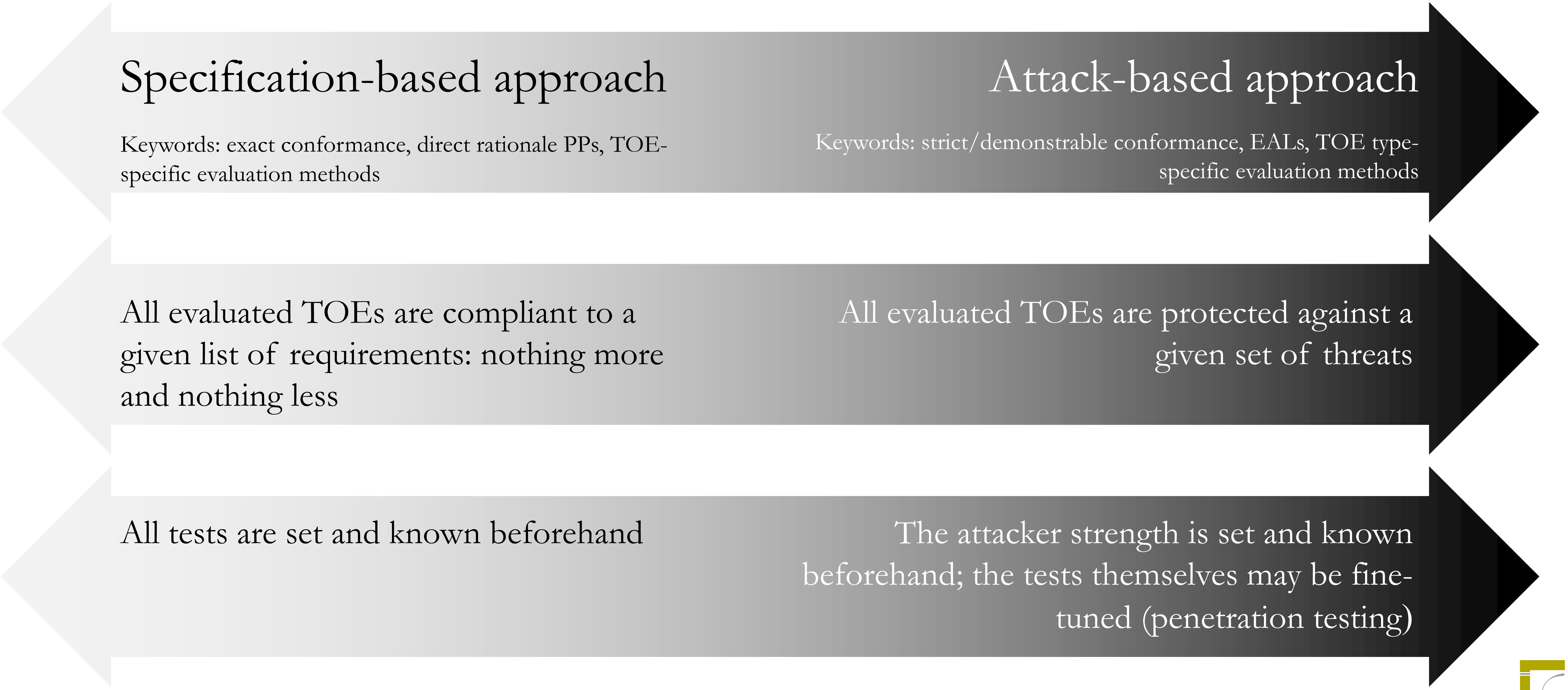
Content Overview

TR 22216 Clause 5



← Exact conformance

Security evaluation - Two approaches



Specification-based approach

Keywords: exact conformance, direct rationale PPs, TOE-specific evaluation methods

Attack-based approach

Keywords: strict/demonstrable conformance, EALs, TOE type-specific evaluation methods

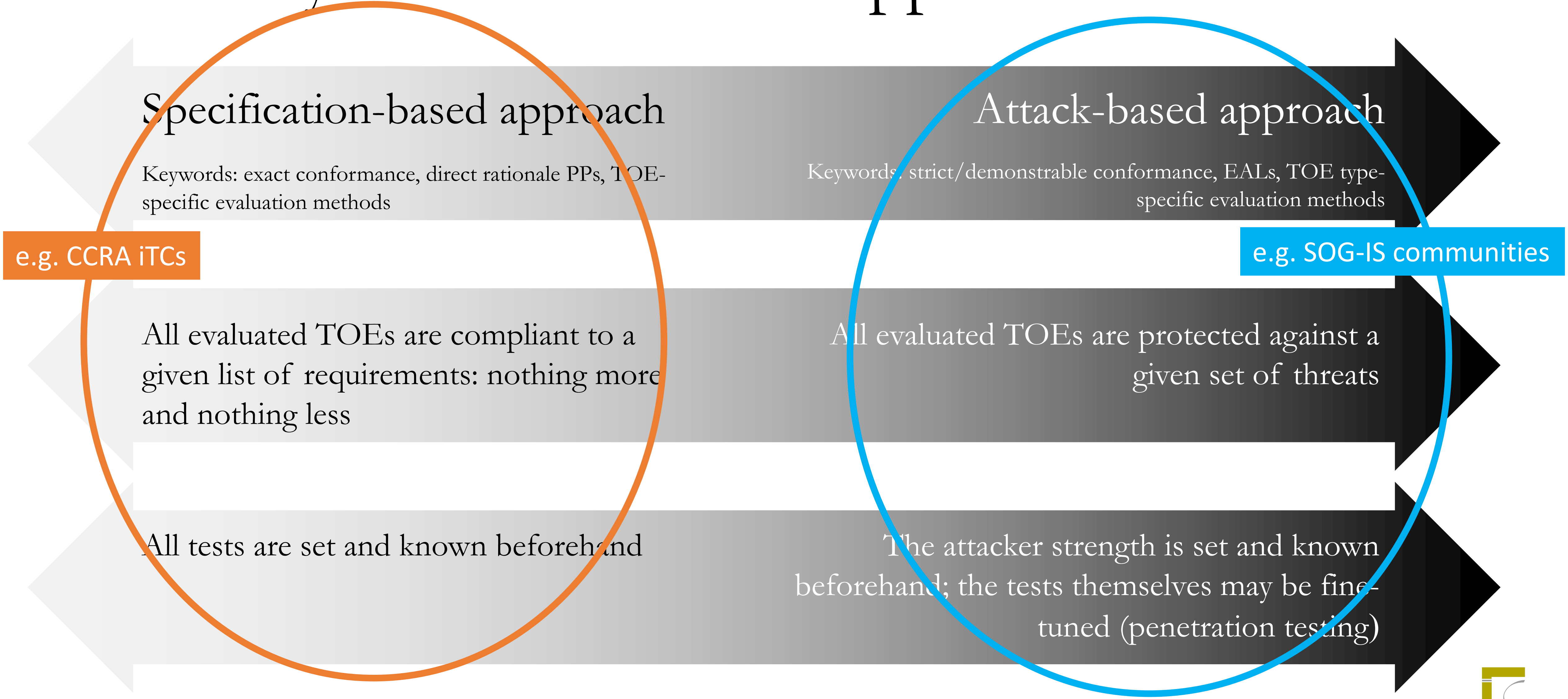
All evaluated TOEs are compliant to a given list of requirements: nothing more and nothing less

All evaluated TOEs are protected against a given set of threats

All tests are set and known beforehand

The attacker strength is set and known beforehand; the tests themselves may be fine-tuned (penetration testing)

Security evaluation - Two approaches



Specification-based approach

Keywords: exact conformance, direct rationale PPs, TOE-specific evaluation methods

Attack-based approach

Keywords: strict/demonstrable conformance, EALs, TOE type-specific evaluation methods

e.g. CCRA iTCs

e.g. SOG-IS communities

All evaluated TOEs are compliant to a given list of requirements: nothing more and nothing less

All evaluated TOEs are protected against a given set of threats

All tests are set and known beforehand

The attacker strength is set and known beforehand; the tests themselves may be fine-tuned (penetration testing)

Content Overview

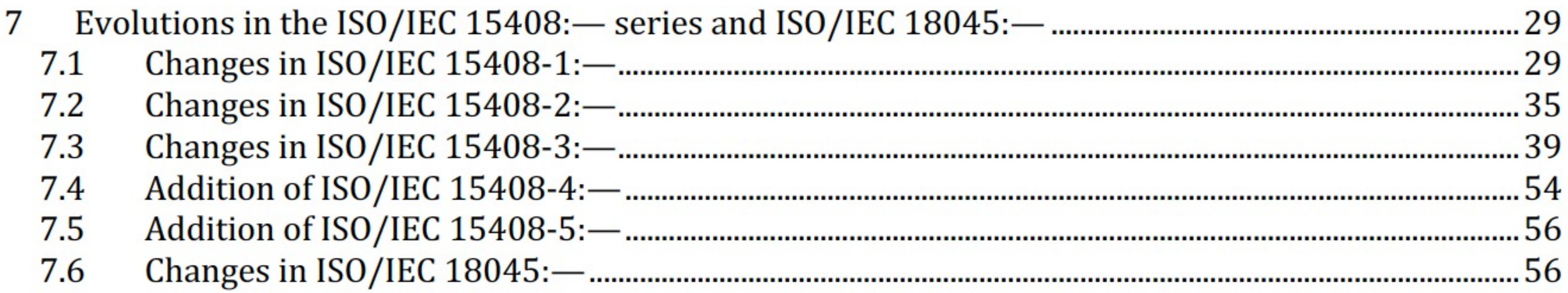
TR 22216 Clause 6

Applying the ISO/IEC 15408 series to specific needs

- Refining and deriving requirements
- Refining and deriving evaluation methods

Content Overview

TR 22216 Clause 7

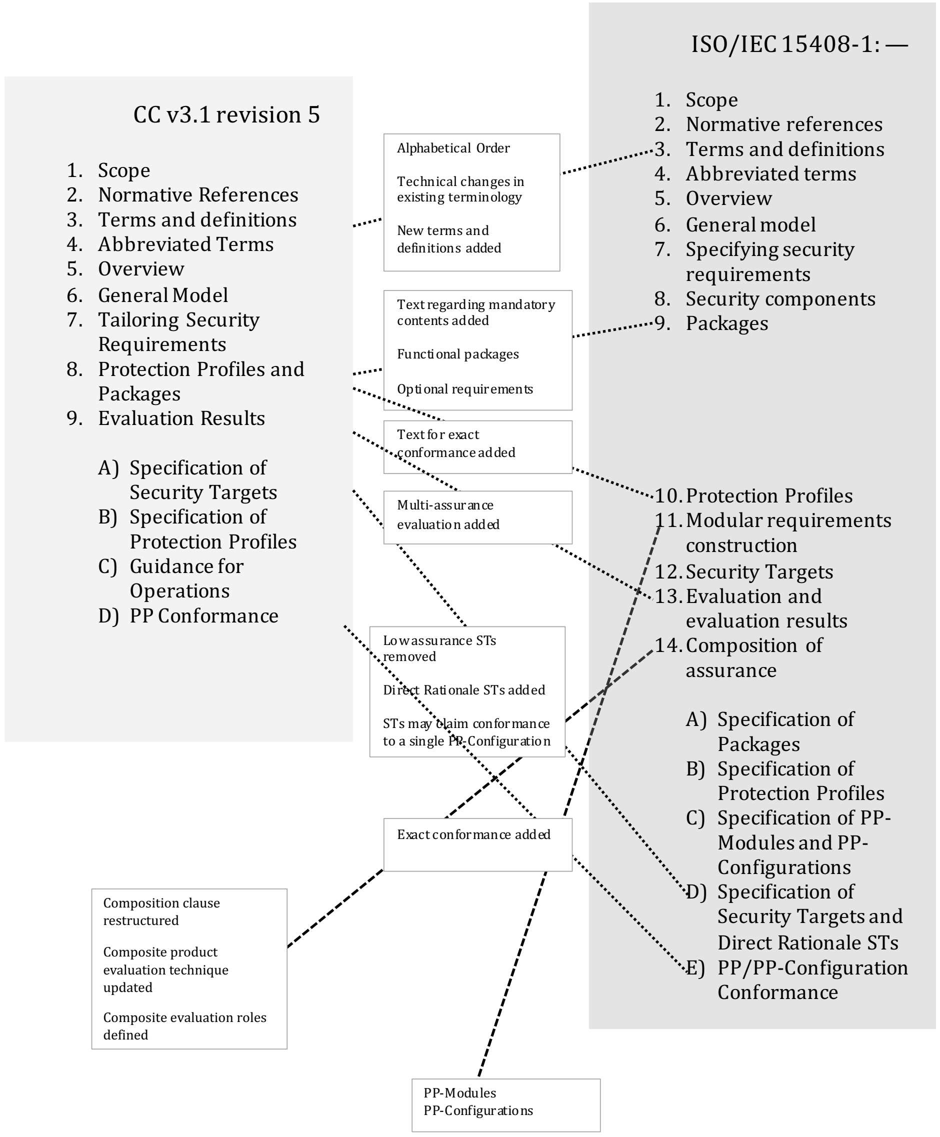


- Tables and diagrams summarize the changes or new content of each part
- Changes are mapped to CC v3.1

Content Overview

TR 22216 Clause 7.1

- Table with new/modified concepts in ISO/IEC 15408-1
- Changes are mapped to CC v3.1



CC v3.1 revision 5

1. Scope
2. Normative References
3. Terms and definitions
4. Abbreviated Terms
5. Overview
6. General Model
7. Tailoring Security Requirements
8. Protection Profiles and Packages
9. Evaluation Results

A) Specification of Security Targets
B) Specification of Protection Profiles
C) Guidance for Operations
D) PP Conformance

Alphabetical Order

Technical changes in existing terminology

New terms and definitions added

Text regarding mandatory contents added

Functional packages

Optional requirements

Text for exact conformance added

Multi-assurance evaluation added

Low assurance STs removed

Direct Rationale STs added

STs may claim conformance to a single PP-Configuration

Exact conformance added

Composition clause restructured

Composite product evaluation technique updated

Composite evaluation roles defined

PP-Modules
PP-Configurations

ISO/IEC 15408-1: —

1. Scope
2. Normative references
3. Terms and definitions
4. Abbreviated terms
5. Overview
6. General model
7. Specifying security requirements
8. Security components
9. Packages
10. Protection Profiles
11. Modular requirements construction
12. Security Targets
13. Evaluation and evaluation results
14. Composition of assurance

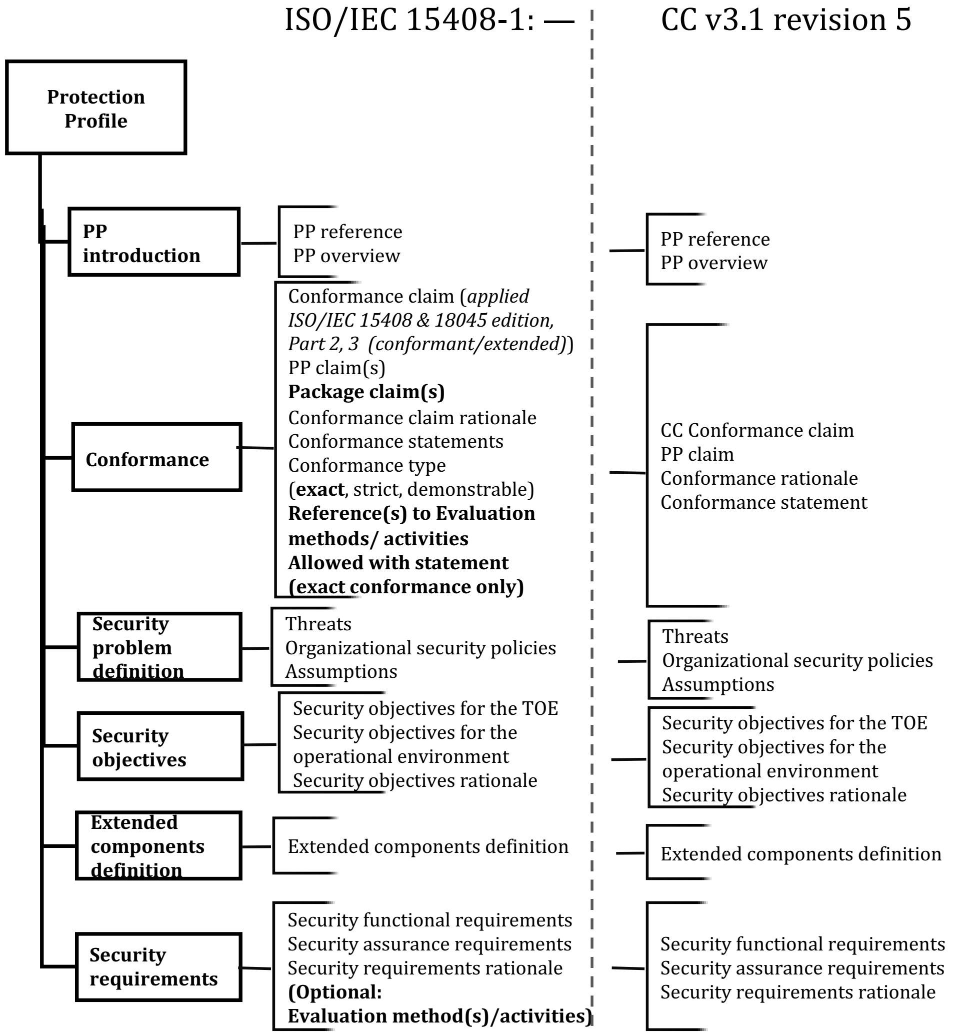
A) Specification of Packages
B) Specification of Protection Profiles
C) Specification of PP-Modules and PP-Configurations
D) Specification of Security Targets and Direct Rationale STs
E) PP/PP-Configuration Conformance

Content Overview

TR 22216 Clause 7.1

- Diagrams showing the differences between the mandatory contents of PPs, STs, PP-Modules and PP-Configurations in CC v3.1 and the 4th edition of ISO/IEC 15408-1

Contents of a Protection Profile



ISO/IEC 15408-1: —

CC v3.1 revision 5

Protection Profile

PP introduction

PP reference
PP overview

PP reference
PP overview

Conformance

Conformance claim (*applied ISO/IEC 15408 & 18045 edition, Part 2, 3 (conformant/extended)*)
PP claim(s)
Package claim(s)
Conformance claim rationale
Conformance statements
Conformance type
(**exact**, strict, demonstrable)
Reference(s) to Evaluation methods/ activities
Allowed with statement (exact conformance only)

CC Conformance claim
PP claim
Conformance rationale
Conformance statement

Security problem definition

Threats
Organizational security policies
Assumptions

Threats
Organizational security policies
Assumptions

Security objectives

Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale

Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale

Extended components definition

Extended components definition

Extended components definition

Security requirements

Security functional requirements
Security assurance requirements
Security requirements rationale
(Optional: Evaluation method(s)/activities)

Security functional requirements
Security assurance requirements
Security requirements rationale

Content Overview

TR 22216 Clause 7.2

- Changes to the SFRs are illustrated

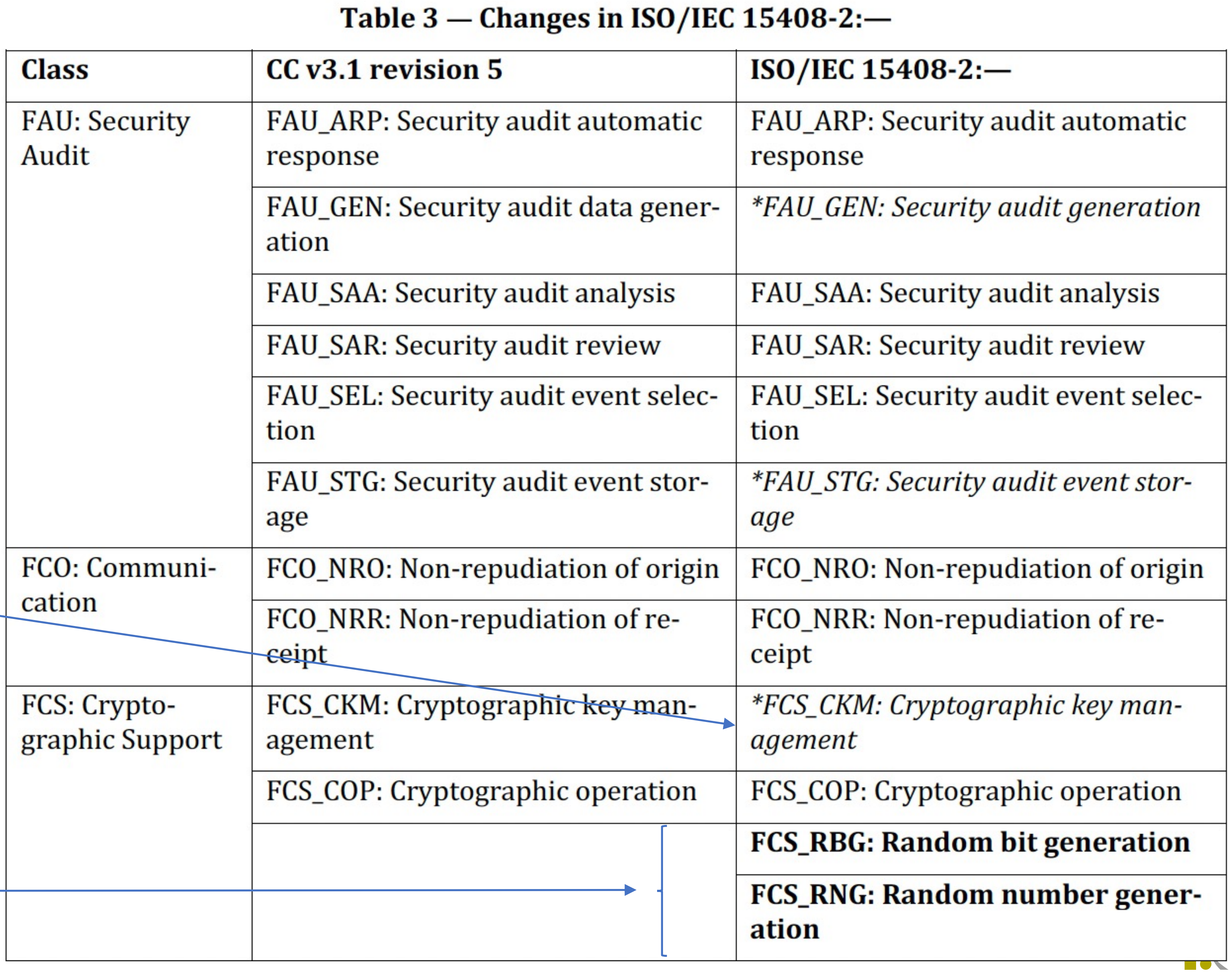


Table 3 — Changes in ISO/IEC 15408-2:—

Class	**CC v3.1 revision 5**	**ISO/IEC 15408-2:—**
FAU: Security Audit	FAU_ARP: Security audit automatic response	FAU_ARP: Security audit automatic response
	FAU_GEN: Security audit data generation	*FAU_GEN: Security audit generation
	FAU_SAA: Security audit analysis	FAU_SAA: Security audit analysis
	FAU_SAR: Security audit review	FAU_SAR: Security audit review
	FAU_SEL: Security audit event selection	FAU_SEL: Security audit event selection
	FAU_STG: Security audit event storage	*FAU_STG: Security audit event storage
FCO: Communication	FCO_NRO: Non-repudiation of origin	FCO_NRO: Non-repudiation of origin
	FCO_NRR: Non-repudiation of receipt	FCO_NRR: Non-repudiation of receipt
FCS: Cryptographic Support	FCS_CKM: Cryptographic key management	*FCS_CKM: Cryptographic key management
	FCS_COP: Cryptographic operation	FCS_COP: Cryptographic operation
		FCS_RBG: Random bit generation
		FCS_RNG: Random number generation

Updated

Newly introduced

Content Overview

TR 22216 Clause 7.3

- Important changes and additions to each class are illustrated
- Tables for APE, ACE, ASE, ADV, AGD, ALC, ATE, AVA, ACO

Updated

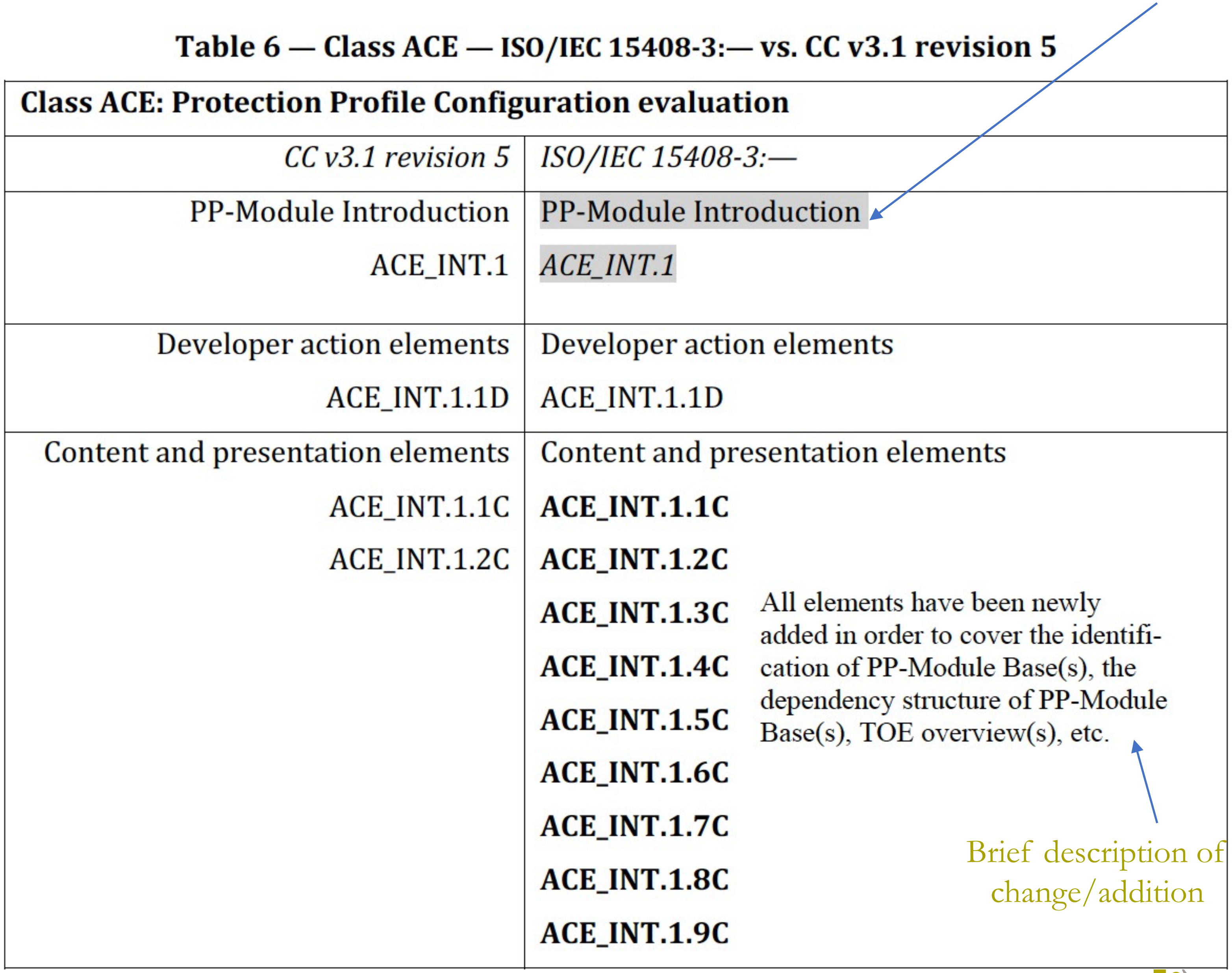


Table 6 — Class ACE — ISO/IEC 15408-3:— vs. CC v3.1 revision 5

Class ACE: Protection Profile Configuration evaluation		
CC v3.1 revision 5	*ISO/IEC 15408-3:—*	
PP-Module Introduction	PP-Module Introduction	
ACE_INT.1	*ACE_INT.1*	
Developer action elements	Developer action elements	
ACE_INT.1.1D	ACE_INT.1.1D	
Content and presentation elements	Content and presentation elements	
ACE_INT.1.1C	**ACE_INT.1.1C**	
ACE_INT.1.2C	**ACE_INT.1.2C**	
	ACE_INT.1.3C	All elements have been newly added in order to cover the identification of PP-Module Base(s), the dependency structure of PP-Module Base(s), TOE overview(s), etc.
	ACE_INT.1.4C	
	ACE_INT.1.5C	
	ACE_INT.1.6C	
	ACE_INT.1.7C	
	ACE_INT.1.8C	
	ACE_INT.1.9C	

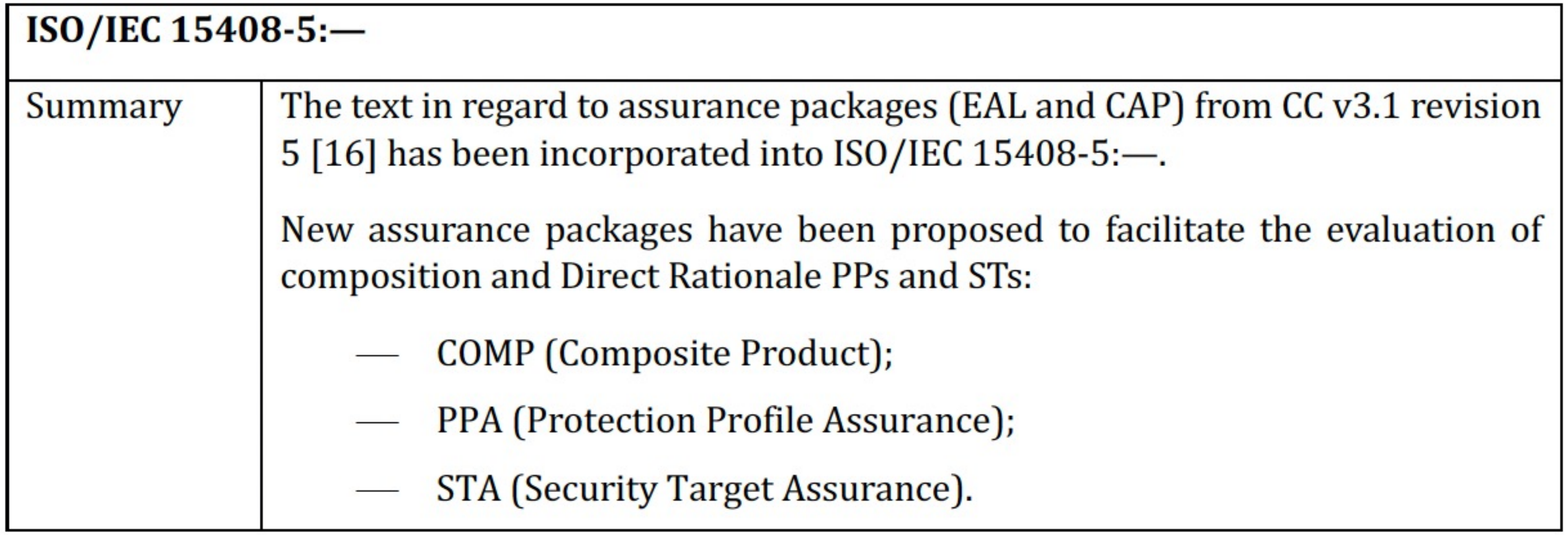
Brief description of change/addition

Content Overview

TR 22216 Clause 7.4 & 7.5

- For ISO/IEC 15408-4 & 5 and ISO/IEC 18045, a table summarizing the contents is included

Table 15 — ISO/IEC 15408-5:—



ISO/IEC 15408-5:—	
Summary	The text in regard to assurance packages (EAL and CAP) from CC v3.1 revision 5 [16] has been incorporated into ISO/IEC 15408-5:—. New assurance packages have been proposed to facilitate the evaluation of composition and Direct Rationale PPs and STs: — COMP (Composite Product); — PPA (Protection Profile Assurance); — STA (Security Target Assurance).

Documents Navigation - Tips

Experienced CC Users

EC 15408 & ISO/IEC 18045

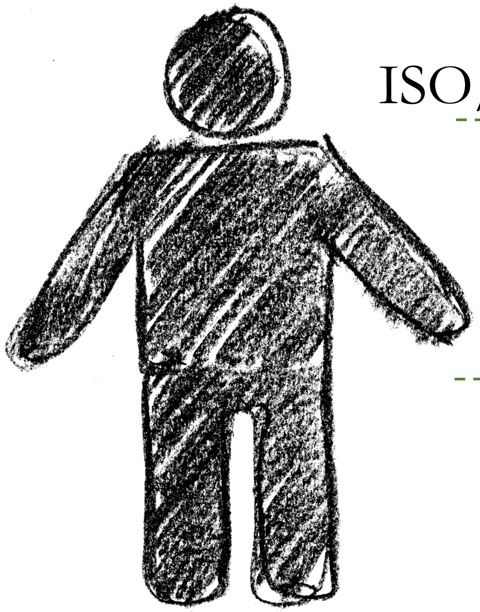
- Compatibility with existing practices and processes
- Expanded toolbox for the security specification and evaluation methodology

TR 22216

- Summary of relevant changes
- Mapping to CC v3.1

Documents Navigation - Tips

New CC Users



ISO/IEC 15408 & ISO/IEC 18045

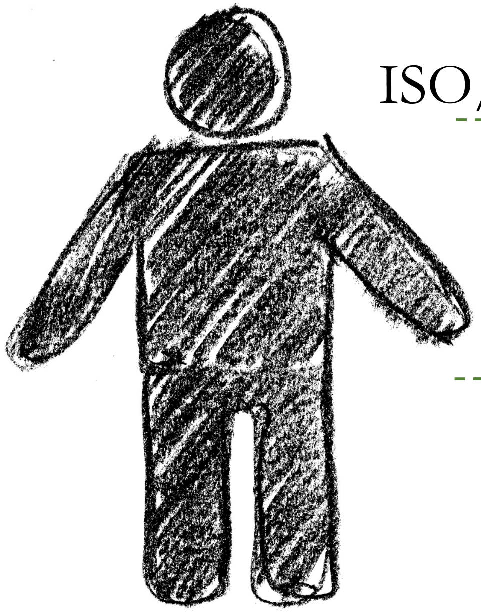
- Expanded toolbox for the security specification and evaluation methodology

TR 22216

- Overview of standard structure
- Summary of content and evaluation approaches
- Guidance on using the standard for specific needs

Documents Navigation - Tips

Risk owners / Developers



ISO/IEC 15408 & ISO/IEC 18045

- Identify security requirements to be satisfied by their TOE
- Determine responsibilities and actions regarding evidence that is necessary to support the evaluation of the TOE against these requirements
- Guidance on structure of PP/PP-Modules/PP-Configurations/STs, etc.

TR 22216

- Clause 1 and Clause 5 introduce and describe new concepts and features
- In clause 7.1, the diagrams illustrate the changes to the structure of PP/PP-Modules/PP-Configurations/STs
- In clause 7.3, the included table contains potential changes to the developer elements

Documents Navigation - Tips

Evaluators

EC 15408 & ISO/IEC 18045

- Criteria to be used when forming judgements about the conformance of TOEs, STs, PPs and PP-Configurations to their security requirements
- General set of actions to be carried out

TR 22216

- Overview for identifying relevant information
- Clauses 7.2 and 7.3 provide tables identifying and illustrating updated/new SFRs and SARs

Conclusion

- The fourth edition of the ISO/IEC 15408 series and ISO/IEC 18045:
  - Includes substantial changes and additions for addressing the evaluation of complex products and supporting the needs of different user communities
  - Ensures compatibility with currently existing practices and processes

- The Transition Guide TR22216 was developed simultaneously with the new edition. It aims to support the transition to the new edition smoothly by
  - Providing a general view of the fourth edition
  - Summarizing the new concepts and related evaluation approaches.

Acknowledgements

- SC27 WG3 expert team
- Specially
  - Elżbieta Andrukiewicz
  - Fiona Pattinson
  - Miguel Bañon
  - Naruki Kai

INTERNET
OF TRUST