Conformity Assessment

Christoph Herbst

# SECURE PRODUCT LIFECYLE

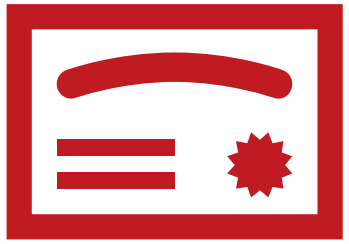


Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# Agenda

- Security Certification & Legal Framework
- Security Testing

- Common Criteria
  - Security Target and Protection Profile
  - Security Requirements – Organization and Operations
  - Security functional requirements (SFR)
  - Security assurance requirements (SAR)
  - Evaluation Assurance Levels (EAL)



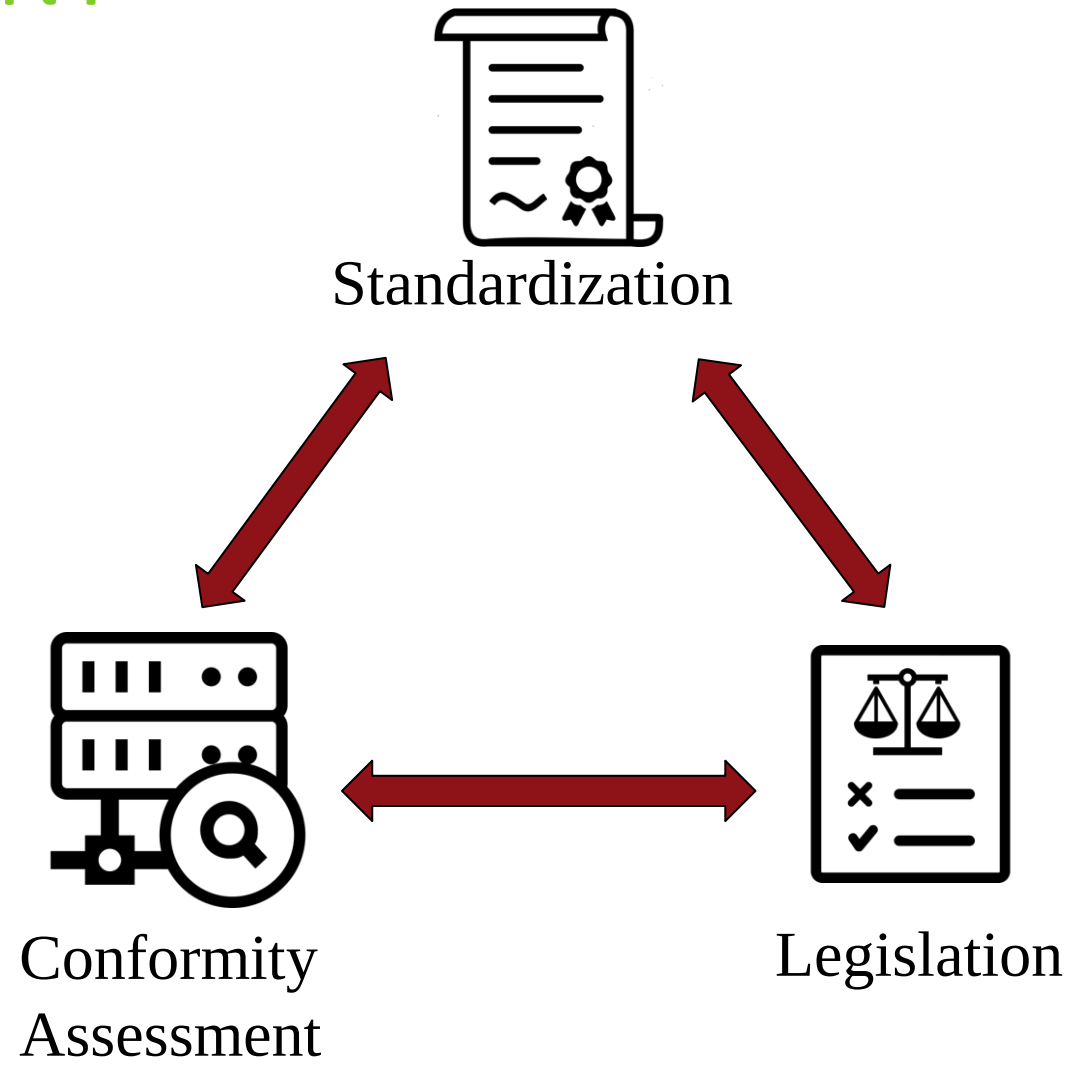
Security Certification &

Legal Framework



Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# TRUST THROUGH CONFORMITY ASSESSMENT

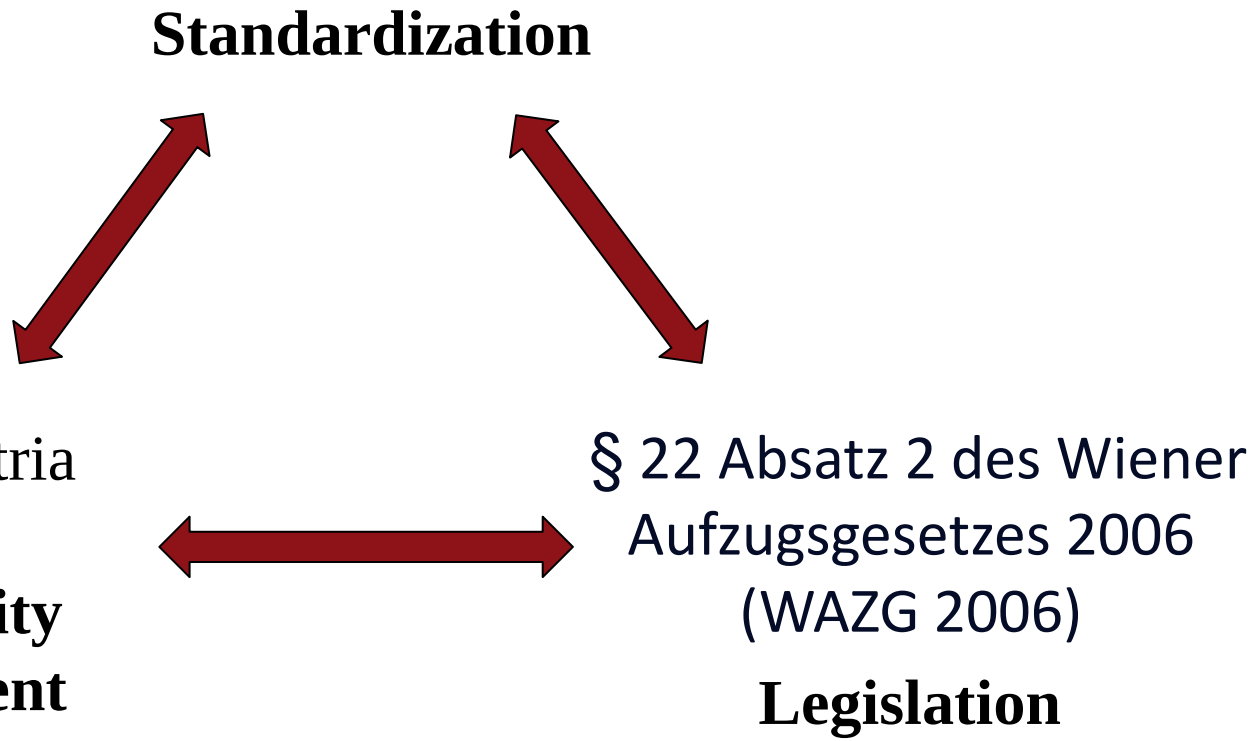




In force since 27th of June 2019

# CONFORMITY ASSESSMENT
# e.g. Elevator

ÖNORM B 2476-1:2011-11-15
bzw. ÖNORM B 2476-2:2016-05-01



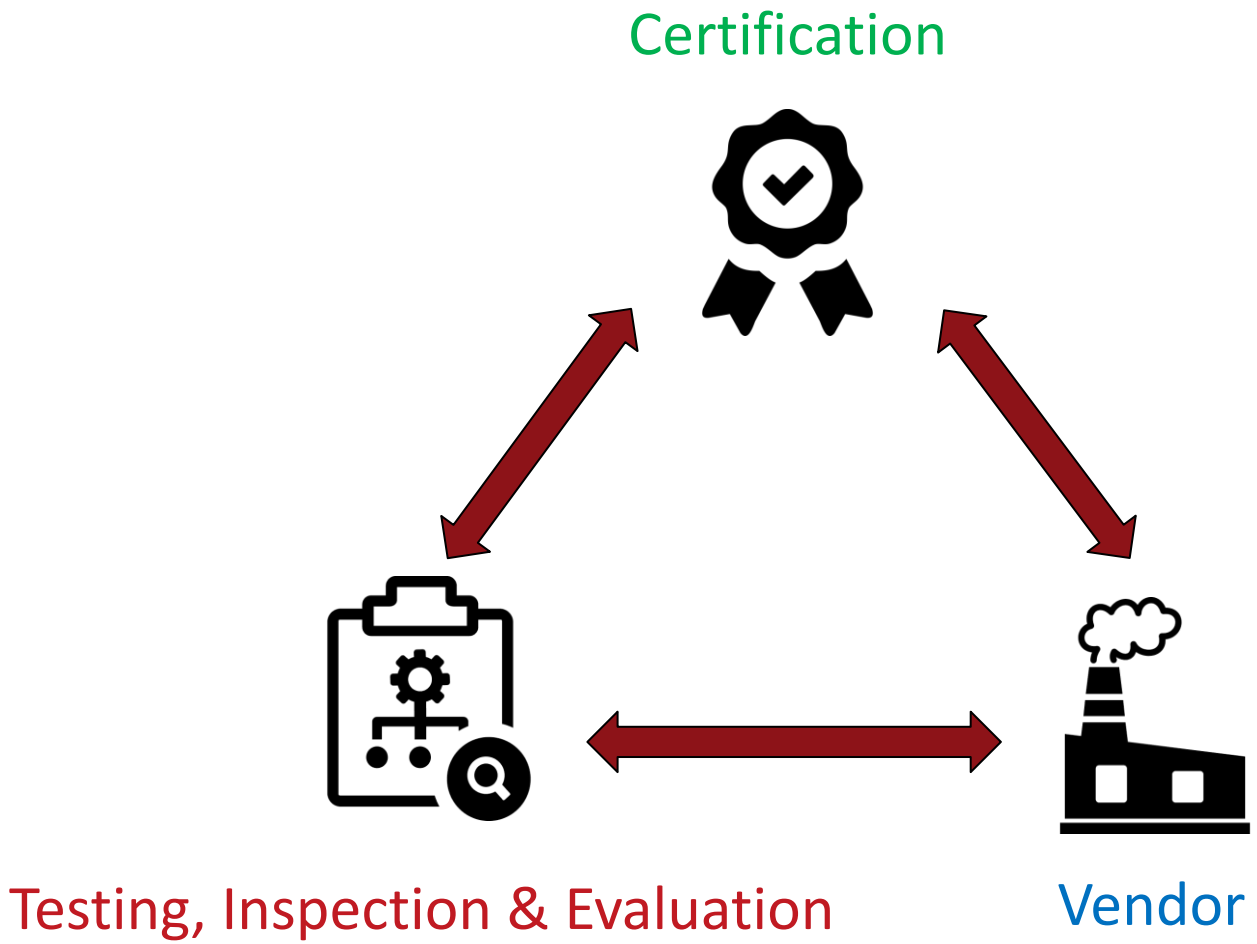
# CONFORMITY ASSESSMENT
# A New Challenge

- Definition according to EN ISO/IEC 17000:2004
  - *“Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”*

- Traditional setup
  - Criteria are usually static: physical laws do not change
  - Check-list approach

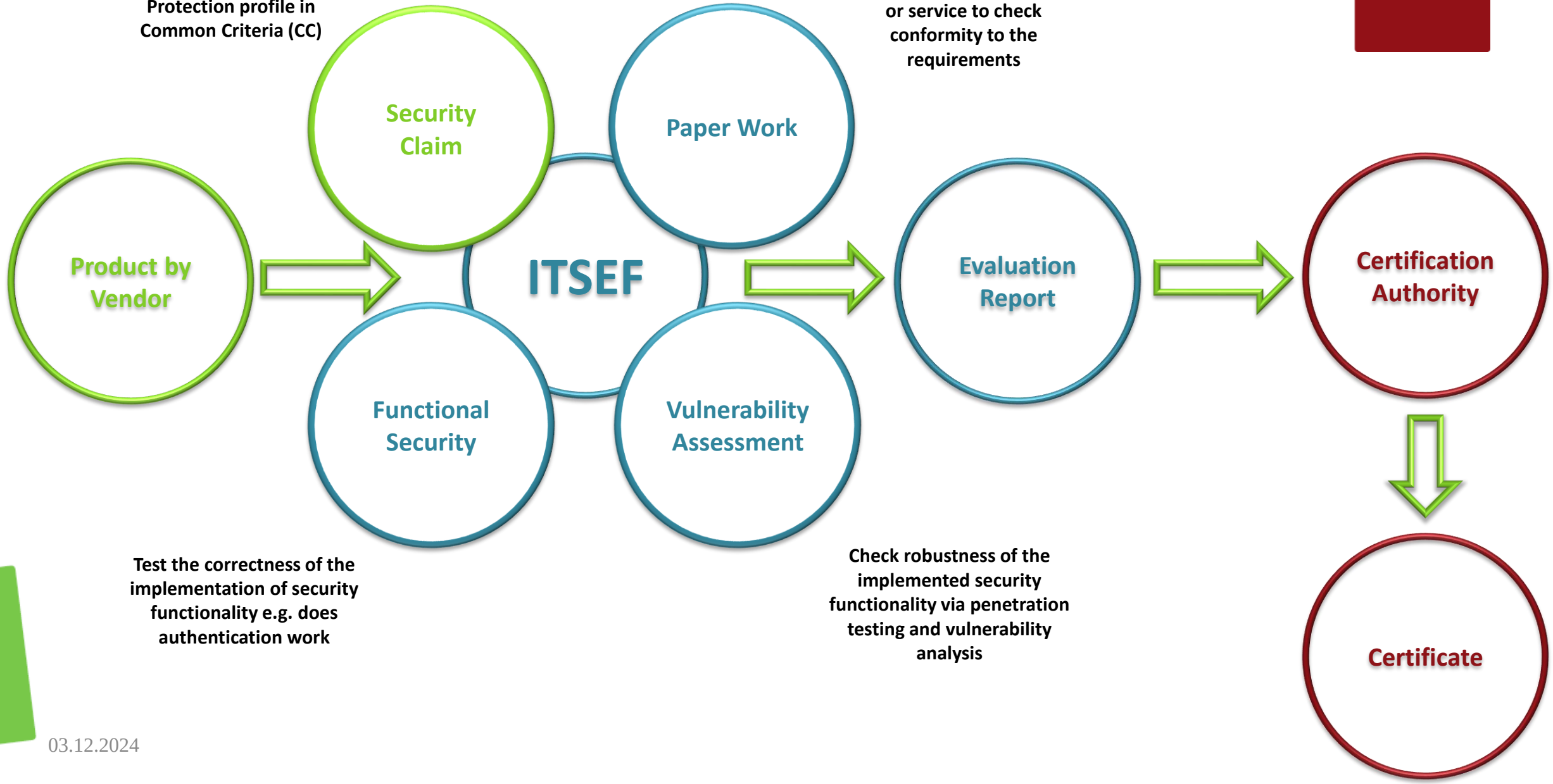
- Cybersecurity setup
  - Criteria are dynamic: Attacks are evolving
  - Check-list approach („security functional compliance“) vs. asset-based vulnerability assessment approach („security robustness“)
  - Assurance level based approach

# Certification Framework



The requirements given by a standard or self defined for a certain product. E.g. Protection profile in Common Criteria (CC)

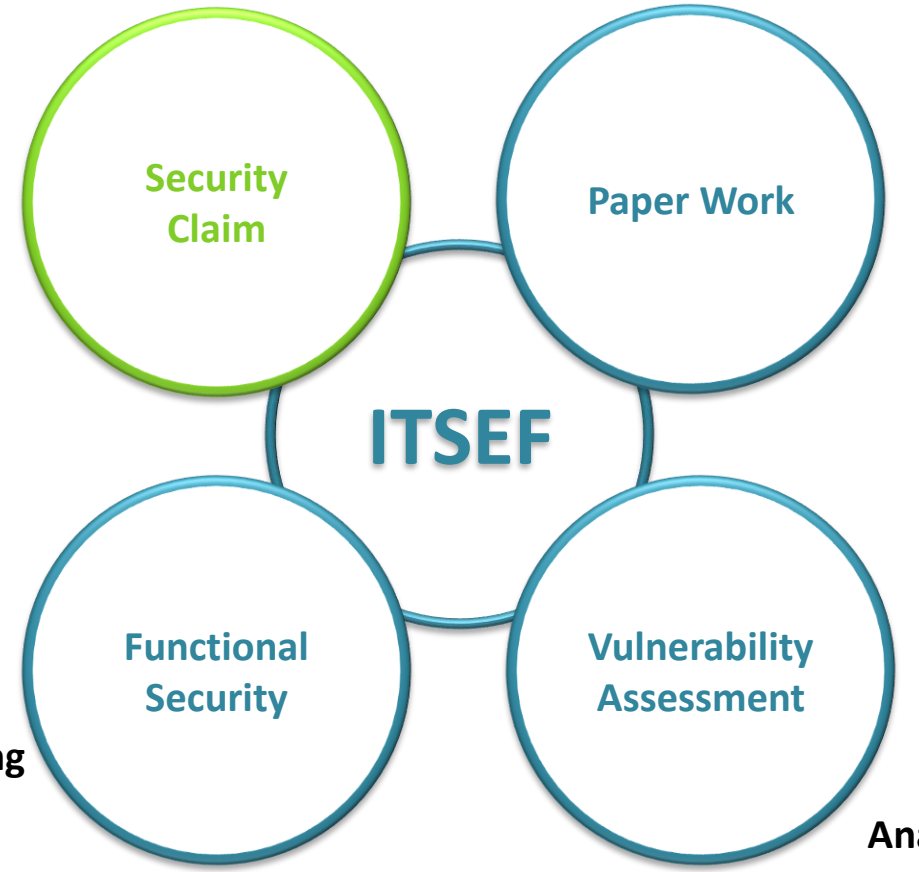
Work done by an evaluation facility to check technical documentation of a product or service to check conformity to the requirements




Test the correctness of the implementation of security functionality e.g. does authentication work

Check robustness of the implemented security functionality via penetration testing and vulnerability analysis

In CC written by vendor, in other schemes partially given (via a fixed specification/standard for a use case)

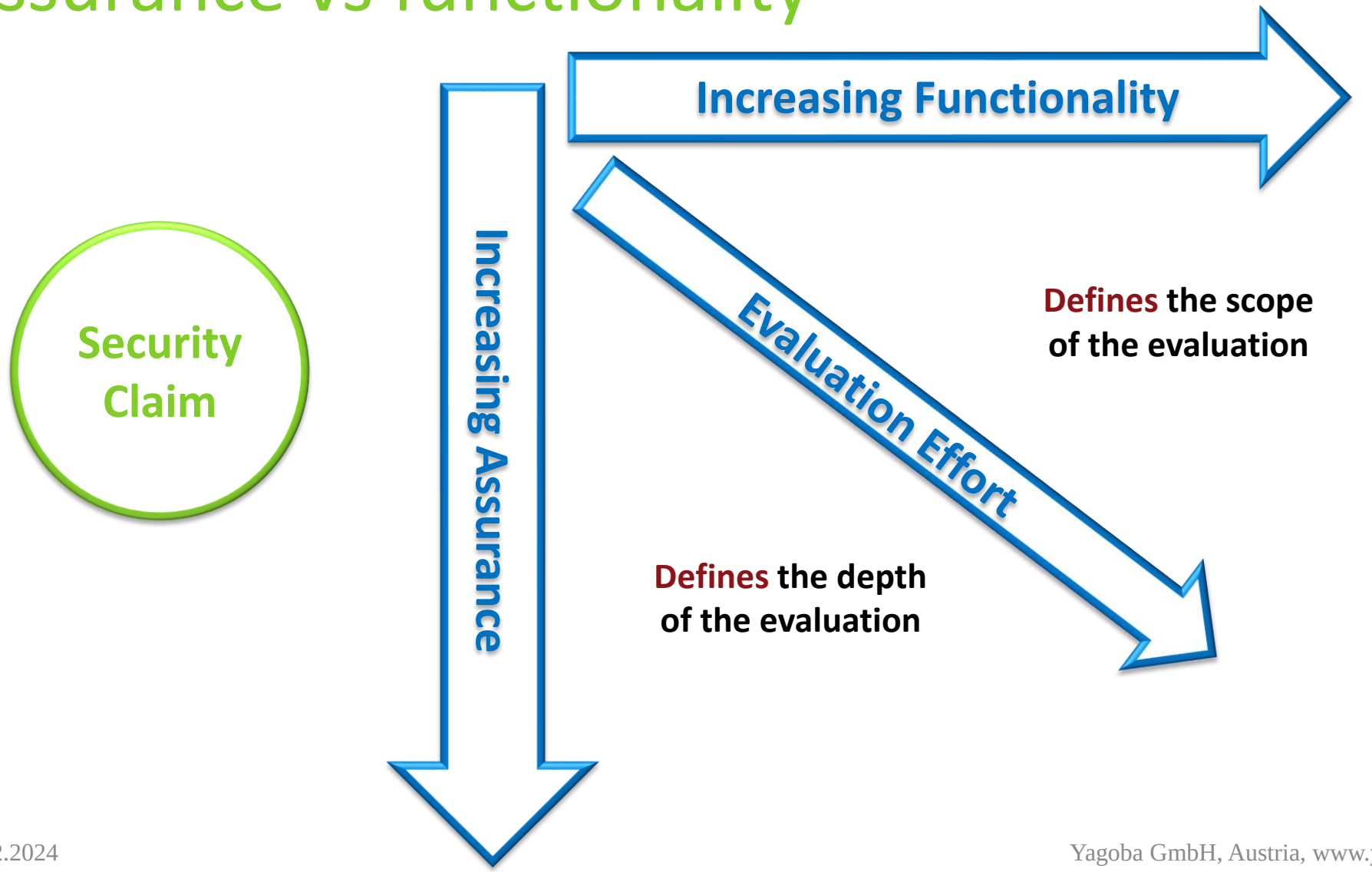



CC: hundreds to thousands of pages
Lightweight schemes: up to hundred

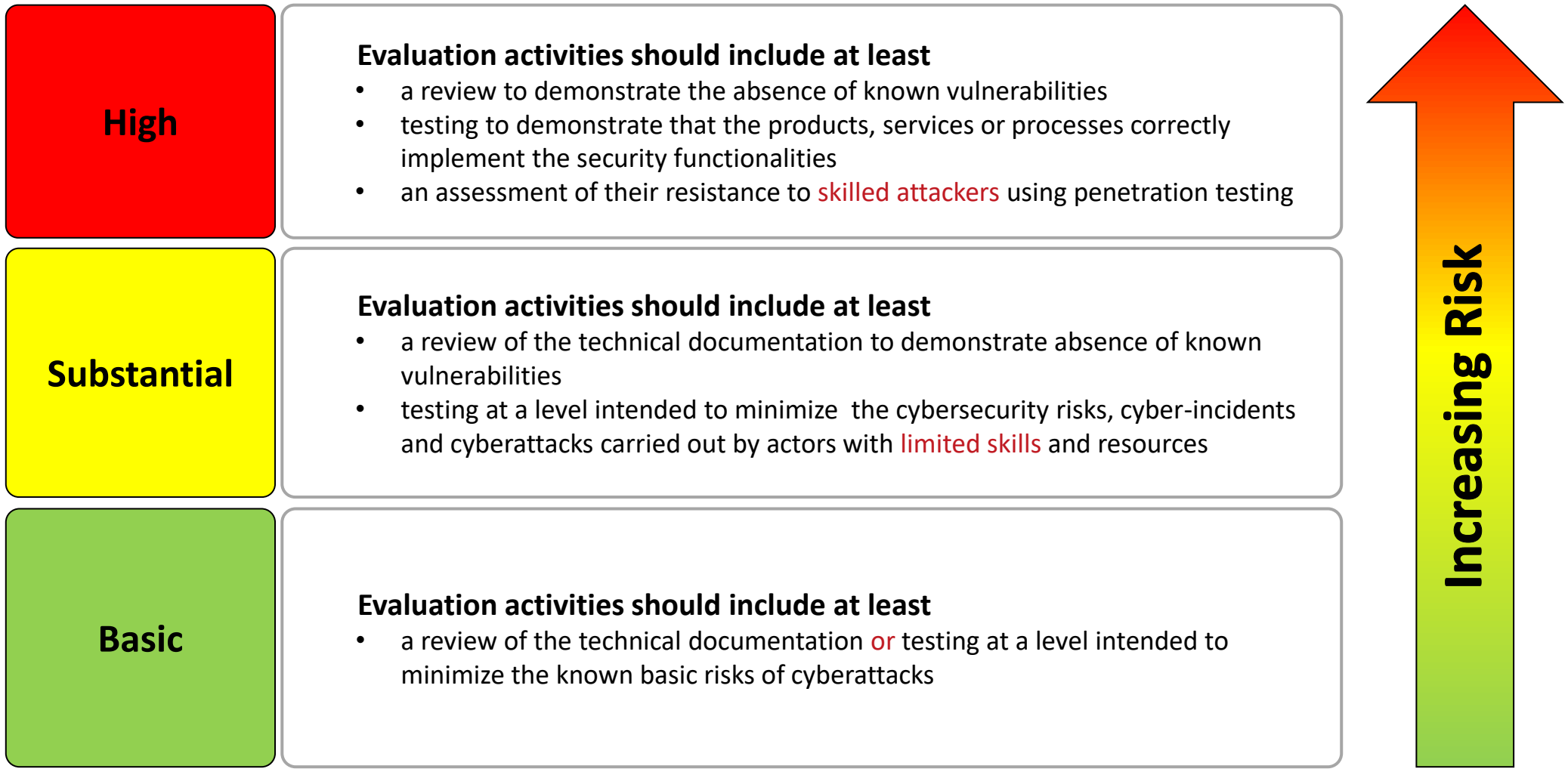
CC: Independent functional testing
Lightweight schemes: Strongly depends on the scheme

CC: Implementation review, Vulnerability Analysis (VA) Plan, VA Testing (e.g. Penetration Testing) up to several months effort
Lightweight schemes: Timeboxed e.g 15 days

# Security Claim
# Assurance vs functionality



# Assurance Levels



# Governmental Stakeholders preparing for stringent regulation




*There is a huge gap on trust on the digital market. Industrial and governmental stakeholders are taking action strengthening regulation across all regions …*

- EU Cybersecurity Act being in force since June 27th 2019
  - establishes an EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services.
  - The EU Cybersecurity Act revamps and strengthens the EU Agency for cybersecurity (ENISA).
  - Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the EU.
- GDPR being effective since May 2018
  - The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). The GDPR aims primarily to give control to individuals over their personal data.
- California Consumer Privacy Act (2018)
  - The California Consumer Privacy Act (CCPA) is a bill intended to enhance privacy rights and consumer protection for residents of California. The bill was signed into law on June 28, 2018. The CCPA becomes effective on January 1, 2020.
- California Bills: SB 327 & AB 1906
  - Starting on January 1st, 2020, any manufacturer of a device that connects “directly or indirectly” to the internet must equip it with “reasonable” security features, designed to prevent unauthorized access, modification, or information disclosure.
- Common Criteria
  - CCRA and SOGIS being in place since years and build up to now the backbone of cross-recognized international security certification

SOGIS
Recognition Agreement

# IoT Cybersecurity Standards & Regulation Examples - No complete list

**Widely accepted standards, specifications & guidances:**

- GSMA: IoT Security Guidelines
- IoT Security Foundation: IoT Security Compliance Framework & Secure Design Best Practice Guides and more

**Standards tackling security maturity of organisations/industry 4.0:**

- IEC 62443 Family: *Security for industrial automation and control systems*
- ISO/IEC 27001: *Information technology – Security techniques – Information security management systems*

**US centric:**

Regulation:

- Federal Trade Commission Act (FTC Act)
- CCPA: The California Consumer Privacy Act (2018)
- California Bills: SB 327 & AB 1906: reasonable security features for connected products
- Children's Online Privacy Protection Act (COPPA)
- Internet of Things (IoT) Cybersecurity Improvement Act

Standards / Specifications:

- UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

Best Practices:

- NIST Cybersecurity Framework
- NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Certification:

- CTIA: IoT Cybersecurity Certification Program

**EU centric:**

Regulation:

- CE Marking
- GDPR regulation (effective since May 2018)
- EU Cybersecurity Act defining an EU-wide cybersecurity certification framework (effective since June 2019)

Standards/Specifications:

- ETSI:
  - TS 103 645 & EN 303 645 (Securing Consumer IoT)
  - TS 103 701 (Cybersecurity assessment for IoT products)
  - TS 103 485 (Privacy Assurance and verification)
- DIN SPEC 27072

Best Practices / Guidance Documents:

- IT-Grundschutz, SYS4.4. IoT Devices (BSI)
- ENISA
  - Good Practices for Security of IoT in the context of Smart Manufacturing (11/2018)
  - Good practices for security of IoT - Secure Software Development Lifecycle (11/2019)
  - Towards secure convergence of Cloud and IoT (09/2018)

# Security Testing



Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# Functional Security VS. Robustness

The secure feature „barrier“ is **functionally correctly** Implemented…

# Functional Security VS. Robustness

The secure feature „barrier“ is **functionally correctly** Implemented…

…but the implementation is **not robust** against attacker not following instructions!

Intro

# COMMON CRITERIA



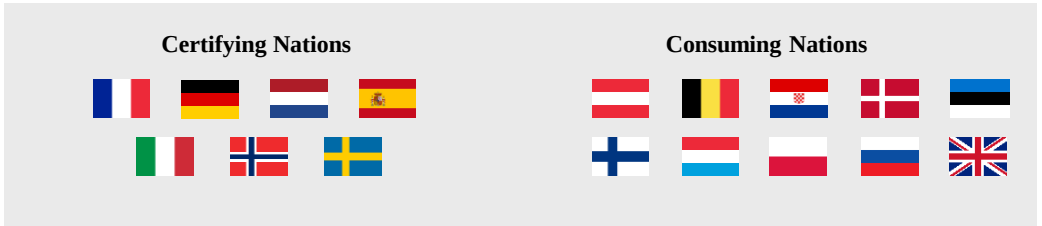
Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# Common Criteria

- Common Criteria for Information Technology Security Evaluation (CC)
- Global criteria for evaluating the assurance of IT products
  - International reconciled tool kit for meaningful security requirements
  - Mutual recognition of CC certificates between different countries
  - Standardized as ISO 15408

Common Criteria Recognition Agreement (CCRA)
global recognition up to EAL2


Senior Officials Group – Information Systems Security (SOG-IS)
European recognition up to EAL4 (TD: EAL7)





Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# Common Criteria

- Common Criteria consist of
  - CC Part 1 Introduction and General Model
  - CC Part 2 Security Functional Requirements (SFRs)
  - CC Part 3 Security Assurance Requirements (SARs)
  - CEM Common Evaluation Methodology
- www.commoncriteriaportal.org

- Common Criteria is further refined by
  - Mandatory National Interpretations by Certification Body
  - Mandatory additions by Technical Domain Working Groups

# Common Criteria

- Common Criteria can be applied to all kinds of IT products
  - Hardware
  - Firmware
  - Software
  - Meaningful combinations of the above
- IT product in scope of an evaluation is called the TOE (Target of Evaluation)
  - The TOE usually also includes the corresponding user guidance
  - The TOE implements the TOE security functionality (TSF)

The requirements selected by the vendor from CC functional and assurance catalogues. A ST can also be derived from one or more Protection Profile(s) (PP).

Work done by an evaluation facility to examine ST, guidance, design, life cycle and test documentation of a product or service to check conformity to the SARs


Test the correctness of the implementation of the SFRs primarily through the developer. This is verified by the evaluator.

Assess robustness of the implemented security functionality via penetration testing and vulnerability analysis against a chosen attack potential

# Security Target


- The Security Target (ST) is the central document defining the (functional and assurance) scope of any CC certification process
- A ST is written for one specific TOE
- Each ST contains the following chapters
  - ST Introduction
  - Conformance Claims
  - Security Problem Definition
  - Security Objectives
  - Extended Component Definition
  - Security Requirements (Functional & Assurance Requirements)
  - TOE Summary Specification

# Protection Profile

- A Protection Profile (PP) is a template for a ST
  - A PP describes a TOE class rather than a specific TOE. Therefore, all TOE specific sections are missing
  - intended to describe a TOE type (e.g. firewalls, smartcards and similar devices, …)
- A PP can be certified
- The same PP is used for many different STs to be used in different evaluations
- STs can claim conformance to one or multiple PPs
- PPs are typically written by:
  - A user community seeking to come to a consensus on the requirements for a given TOE type;
  - A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE;
  - A government or large corporation specifying its requirements as part of its acquisition process.

Functional Requirements & Assurance Requirements

# COMMON CRITERIA



Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# SFR and SAR

- CC Part 2 establishes a set of **functional components (SFRs)** that serve as standard templates upon which to base functional requirements for TOEs.
- CC Part 3 establishes a set of **assurance components (SARs)** that serve as standard templates upon which to base assurance requirements for TOEs.
- CC Part 3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance packages which are called the Evaluation Assurance Levels (EALs).

# Requirements Organization

## Dependencies

- Components can have dependencies to other components.
- If a component depends on one or more other component, these components also need to be included in the ST or PP
- Not fulfilled dependencies need to be explained in the rationale

## Hierarchies

- Components can be hierarchical to other components of the same family
- Hierarchical components fully include and extend the lower component
- A dependency is also fulfilled if a hierarchical higher component is chosen

# Operations

- Components allow operations to be performed on them to tailor them to the TOE

**Assignments**

- allows the specification of parameters
- only permitted where specifically indicated

**Selection**

- allows the specification of one or more items from a list
- only permitted where specifically indicated

**Refinement**

- allows the addition of details
- always permitted

**Iteration**

- allows a component to be used more than once with varying operations
- always permitted

### 12.6.16 FIA_UAU.1 Timing of authentication

**Component relationships**

| | |
|---|---|
| Hierarchical to: | No other components. |
| Dependencies: | FIA_UID.1 Timing of identification |

**FIA_UAU.1.1**

**The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.**

**FIA_UAU.1.2**

**The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

### 12.6.17 FIA_UAU.2 User authentication before any action

**Component relationships**

| | |
|---|---|
| Hierarchical to: | FIA_UAU.1 Timing of authentication |
| Dependencies: | FIA_UID.1 Timing of identification |

**FIA_UAU.2.1**

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

# SFR - Overview

## FAU: Security Audit
- Security audit automatic response (FAU_ARP)
- Security audit data generation (FAU_GEN)
- Security audit analysis (FAU_SAA)
- Security audit review (FAU_SAR)
- Security audit event selection (FAU_SEL)
- Security audit event selection (FAU_SEL)
- Security audit event storage (FAU_STG)

## FIA: Identification and authentication
- Authentication failures (FIA_AFL)
- User attribute definition (FIA_ATD)
- Specification of secrets (FIA_SOS)
- User authentication (FIA_UAU)
- User identification (FIA_UID)
- User-subject binding (FIA_USB)

## FPR: Privacy
- Anonymity (FPR_ANO)
- Pseudonymity (FPR_PSE)
- Unlinkability (FPR_UNL)
- Unobservability (FPR_UNO)

## FCS: Cryptographic support
- Cryptographic key management (FCS_CKM)
- Cryptographic operation (FCS_COP)

## FRU: Resource utilisation
- Fault tolerance (FRU_FLT)
- Priority of service (FRU_PRS)
- Resource allocation (FRU_RSA)

## FPT: Protection of the TSF
- Fail secure (FPT_FLS)
- Availability of exported TSF data (FPT_ITA)
- Confidentiality of exported TSF data (FPT_ITC)
- Integrity of exported TSF data (FPT_ITI)
- Internal TOE TSF data transfer (FPT_ITT)
- TSF physical protection (FPT_PHP)
- Trusted recovery (FPT_RCV)
- Replay detection (FPT_RPL)
- State synchrony protocol (FPT_SSP)
- Time stamps (FPT_STM)
- Inter-TSF TSF data consistency (FPT_TDC)
- Testing of external entities (FPT_TEE)
- Internal TOE TSF data replication consistency (FPT_TRC)
- TSF self test (FPT_TST)

## FMT: Security management
- Management of functions in TSF (FMT_MOF)
- Management of security attributes (FMT_MSA)
- Management of TSF data (FMT_MTD)
- Revocation (FMT_REV)
- Security attribute expiration (FMT_SAE)
- Specification of Management Functions (FMT_SMF)
- Security management roles (FMT_SMR)

## FCO: Communication
- Non-repudiation of origin (FCO_NRO)
- Non-repudiation of receipt (FCO_NRR)

## FDP: User data protection
- Access control policy (FDP_ACC)
- Access control functions (FDP_ACF)
- Data authentication (FDP_DAU)
- Export from the TOE (FDP_ETC)
- Information flow control policy (FDP_IFC)
- Information flow control functions (FDP_IFF)
- Import from outside of the TOE (FDP_ITC)
- Internal TOE transfer (FDP_ITT)
- Residual information protection (FDP_RIP)
- Rollback (FDP_ROL)
- Stored data integrity (FDP_SDI)
- Inter-TSF user data confidentiality transfer protection (FDP_UCT)
- Inter-TSF user data integrity transfer protection (FDP_UIT)

## FTA: TOE access
- Limitation on scope of selectable attributes (FTA_LSA)
- Limitation on multiple concurrent sessions (FTA_MCS)
- Session locking and termination (FTA_SSL)
- TOE access banners (FTA_TAB)
- TOE access history (FTA_TAH)
- TOE session establishment (FTA_TSE)

## FTP: Trusted path/channels
- Inter-TSF trusted channel (FTP_ITC)
- Trusted path (FTP_TRP)

# SFR - Example

Security Problem Definition

**Threat**
A threat agent may read or modify TOE data using functions of the TOE without the proper authorization.

Security Objectives

**Objective for the TOE**
The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.

**FIA_UAU.1 Timing of authentication**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**FIA_UID.1 Timing of identification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Security Requirements

**FIA_UAU.1.1** The TSF shall allow *user identification and get version* on behalf of the user to be performed before the user is authenticated.
**FIA_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**FIA_UID.1.1** The TSF shall allow *get version* on behalf of the user to be performed before the user is identified.
**FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

TOE Summary Specification

**Security Service Authentication**
The TOE identifies users through the username command, which checks if the username exists (FIA_UID.1). If successful, the user is required to authenticate by providing a password (FIA_UAU.1). No action except for get version is permitted before the user was successfully authenticated.

# SAR - Overview

## ASE: Security Target evaluation

- ST introduction (ASE_INT)
- Conformance claims (ASE_CCL)
- Security problem definition (ASE_SPD)
- Security objectives (ASE_OBJ)
- Extended components definition (ASE_ECD)
- Security requirements (ASE_REQ)
- TOE summary specification (ASE_TSS)

## AGD: Guidance documents

- Operational user guidance (AGD_OPE)
- Preparative procedures (AGD_PRE)

## ADV: Development

- Security Architecture (ADV_ARC)
- Functional specification (ADV_FSP)
- Implementation representation (ADV_IMP)
- TSF internals (ADV_INT)
- Security policy modelling (ADV_SPM)
- TOE design (ADV_TDS)

## ALC: Life-cycle support

- CM capabilities (ALC_CMC)
- CM scope (ALC_CMS)
- Delivery (ALC_DEL)
- Development security (ALC_DVS)
- Flaw remediation (ALC_FLR)
- Life-cycle definition (ALC_LCD)
- Tools and techniques (ALC_TAT)

## ATE: Tests

- Coverage (ATE_COV)
- Depth (ATE_DPT)
- Functional tests (ATE_FUN)
- Independent testing (ATE_IND)

## AVA: Vulnerability Assessment

- Vulnerability analysis (AVA_VAN)

## APE: Protection Profile evaluation

- PP introduction (APE_INT)
- Conformance claims (APE_CCL)
- Security problem definition (APE_SPD)
- Security objectives (APE_OBJ)
- Extended components definition (APE_ECD)
- Security requirements (APE_REQ)

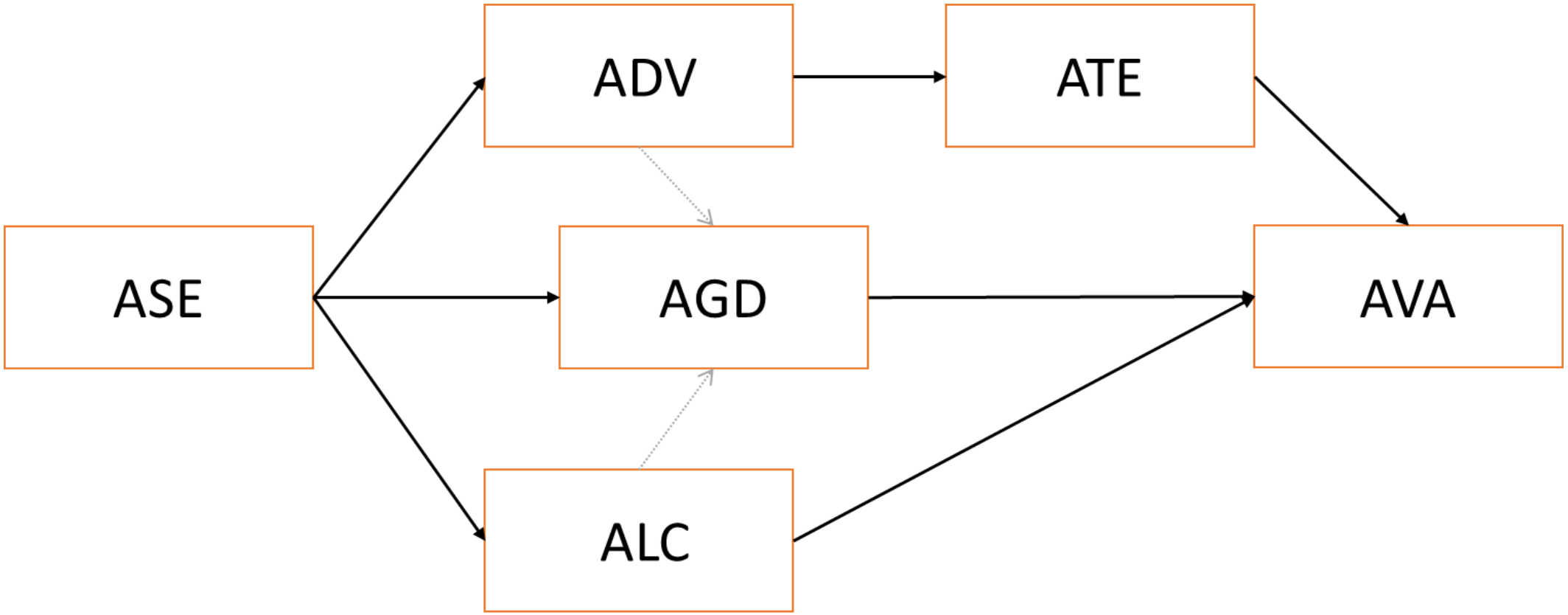
## ACE: Protection Profile configuration evaluation

- PP-Module introduction (ACE_INT)
- PP-Module conformance claims (ACE_CCL)
- PP-Module Security problem definition (ACE_SPD)
- PP-Module Security objectives (ACE_OBJ)
- PP-Module extended components definition (ACE_ECD)
- PP-Module security requirements (ACE_REQ)
- PP-Module consistency (ACE_MCO)
- PP-Configuration consistency (ACE_CCO)

## ACO: Composition

- Composition rationale (ACO_COR)
- Development evidence (ACO_DEV)
- Reliance of dependent component (ACO_REL)
- Composed TOE testing (ACO_CTT)
- Composition vulnerability analysis (ACO_VUL)

# SAR - Typical workflow



# SAR – ASE & AGD

## ASE: Security Target evaluation

- Analyze security target for correctness and consistency

## AGD: Guidance documents

- Analyze operational user guidance for
  - description of secure usage
  - including roles, functions, interfaces and modes of operation
- Analyze preparative user guidance for description of
  - secure set-up
  - instructions for the correct implementation of the objectives for the environment.

# SAR – ADV

- **ADV_FSP (Functional Specification)**
  - Maps the functional specification (SFR's), to the TOE security functionality (TSF) and according interfaces (TSFIs).
  - provides assurance directly by allowing the evaluator to understand how the TSF meets the claimed SFRs
- **ADV_TDS (TOE design)**
  - provides both context for a description of the TSF, and a thorough description of the TSF.
  - provides information to determin that and how the security functional requirements are realized
- **ADV_ARC (Security Architecture)**
  - provides a description of the security architecture of the TSF
  - allows analysis of the information that will confirm the TSF achieves the desired properties
- **ADV_IMP (Implementation representation)**
  - make available the implementation representation (and, at higher levels, the implementation itself) of the TOE in a form that can be analyzed by the evaluator.
- **ADV_INT (TSF internals)**
  - assessment of the internal structure of the TSF if it is well-structured and not overly complex.
- **ADV_SPM (Security policy modelling)**
  - provide additional assurance from the development of a formal security policy model of the TSF

# SAR – ALC

- **ALC_CMC (CM capabilities)**
  - requires the developer's CM system to have capabilities to reduce the likelihood that accidental or unauthorised modifications of the configuration items will occur
  - CM system shall ensure the integrity of the TOE throughout the entire product lifecycle
  - introduces automated CM tools to increase the effectiveness of the CM system and makes it less susceptible to human error or negligence
- **ALC_CMS (CM scope)**
  - identifies items to be included as configuration items and hence placed under ALC_CMC
- **ALC_DEL (Delivery)**
  - Deals with secure transfer of the finished TOE from the development environment into the responsibility of the user
- **ALC_DVS (Development security)**
  - concerned with physical, procedural, personnel, and other security measures used in the development & production environment
  - Usually requires "site visits", i.e. onsite audits of the development and production sites
- **ALC_LCD (Life-cycle definition)**
  - requires that a model for the development and maintenance be established as early as possible in the TOE's life-cycle
  - improves chances that development and maintenance models contribute to the TOE meeting its SFRs
- **ALC_TAT (Tools and techniques)**
  - Is aspect of selecting tools that are used to develop, analyse and implement the TOE.
  - includes requirements to prevent ill-defined, inconsistent or incorrect development tools from being used, including programming languages, documentation, implementation standards, and other parts of the TOE such as supporting runtime libraries.
- **ALC_FLR (Flaw remediation)**
  - requires that discovered security flaws are tracked and corrected by the developer.
  - provides assurance that the TOE will be maintained and supported in the future

# SAR – ATE

- **ATE_IND (Independent testing)**
  - Assures independent functional testing of the TSF
  - requires the evaluator to execute tests
- **ATE_COV (Coverage)**
  - establishes that the TSF has been tested against its functional specification
  - achieved through an examination of developer evidence of correspondence
- **ATE_FUN (Functional tests)**
  - performed by the developer, provides assurance that the tests are performed and documented correctly
  - contributes to providing assurance that the likelihood of undiscovered flaws is relatively small
- **ATE_DPT (Depth)**
  - deals with the level of detail to which the TSF is tested by the developer, based upon increasing depth of information derived from TOE design, implementation representation and security architecture description
  - objective is to counter the risk of missing an error in the development of the TOE

# SAR – AVA

- **AVA_VAN (Vulnerability analysis)**
  - assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE could allow attackers to violate the SFRs
  - deals with the threats that an attacker will be able to discover flaws that will allow unauthorized access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorized capabilities of other users
  - Considers attackers with increasing attack potential
    - AVA_VAN.1/2 resistant to Basic attack potential
    - AVA_VAN.3 resistant to Enhanced-Basic attack potential
    - AVA_VAN.4 resistant to Moderate attack potential
    - AVA_VAN.5 resistant to High attack potential
  - Considered attack vectors include (depending on claimed resistance level)
    - public domain attack vectors
    - Gray/white box penetration testing (“hacking”)
    - Logical testing (Fuzzing)
    - Side-Channel Analysis (timing, power analysis, emanation analysis)
    - HW Fault Injection (Glitching, Laser attacks)
    - Chemical attacks

Assurance Levels

# COMMON CRITERIA



Yagoba GmbH, Austria, www.yagoba.com, info@yagoba.com

# EAL

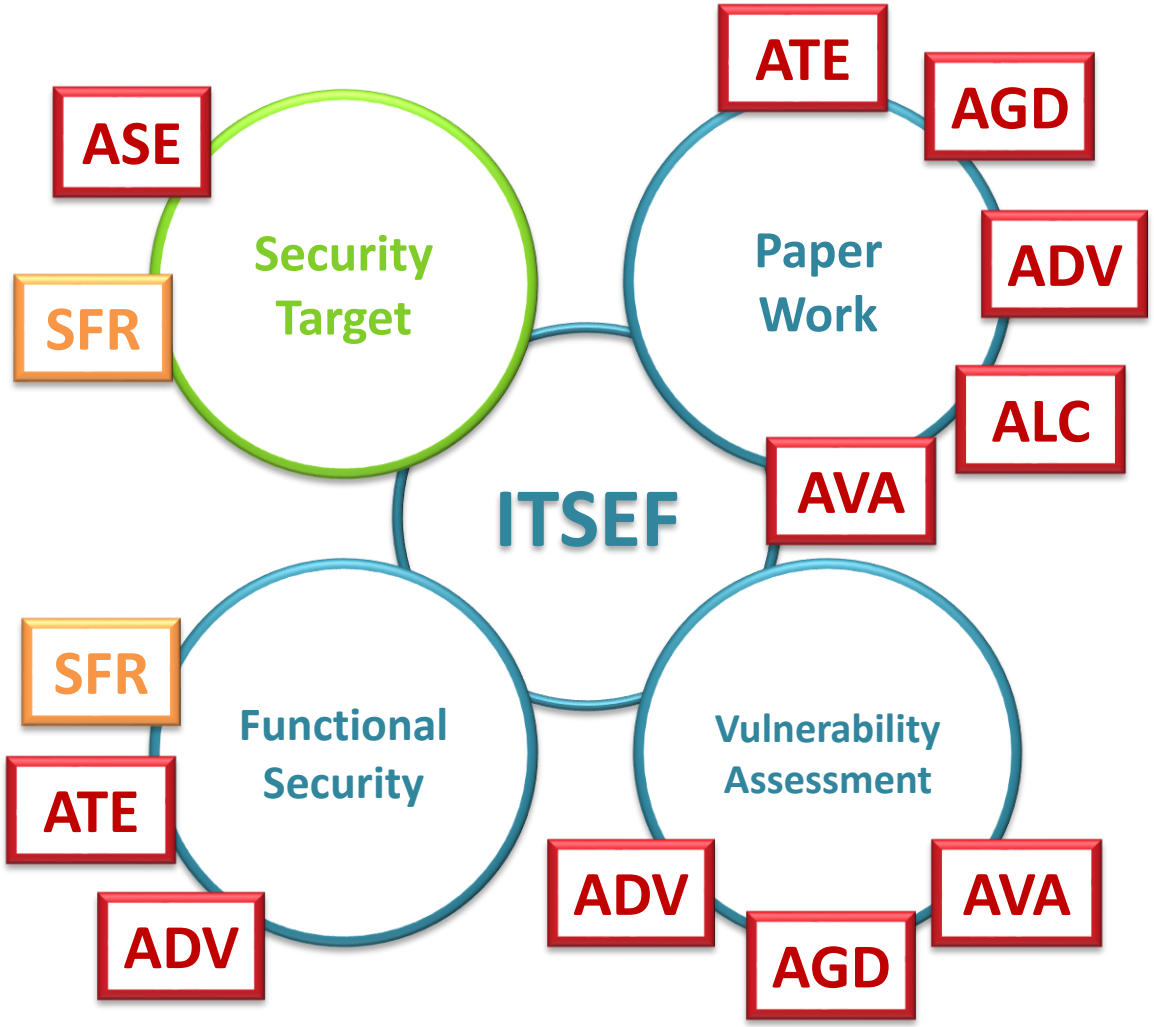
- EALs are predefined packages of assurance components. All predefined packages fulfill the dependencies.
- 7 defined EALs exist, with increasing assurance from 1 to 7
  - EAL1 – functionally tested
  - EAL2 – structurally tested
  - EAL3 – methodically tested and checked
  - EAL4 – methodically designed, tested and reviewed
  - EAL5 – semi formally designed and tested
  - EAL6 – semi formally verified design and tested
  - EAL7 – formally verified design and tested
- Packages can be augmented by additional or hierarchical components, but then the dependencies need to be checked and fulfilled
  - This is denoted with a ‘+’, e.g. EAL4+

# EAL

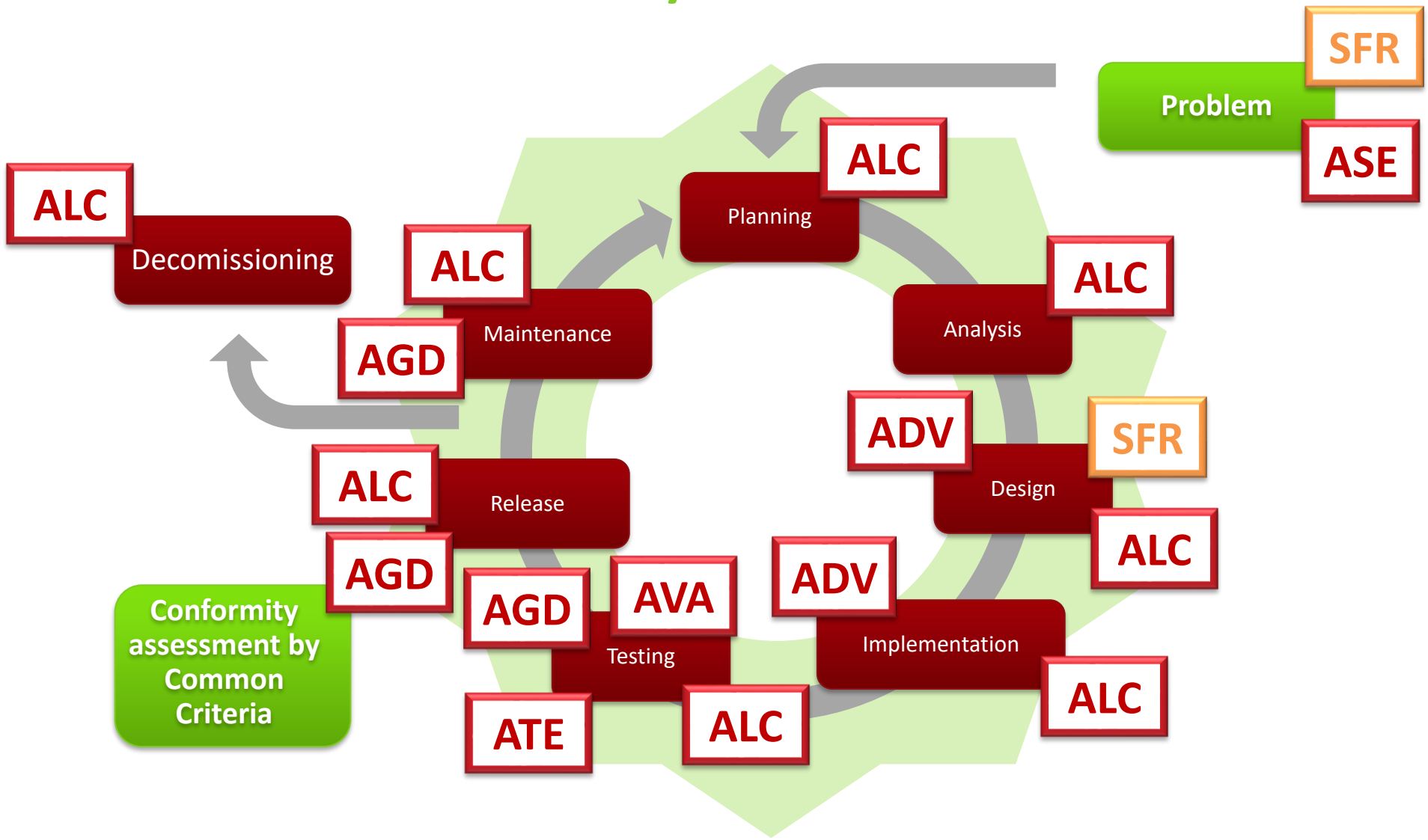
| Assurance class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Development | ADV_ARC | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** |
| | ADV_IMP | | | | **1** | 1 | **2** | 2 |
| | ADV_INT | | | | | **2** | **3** | 3 |
| | ADV_SPM | | | | | | **1** | 1 |
| | ADV_TDS | | **1** | **2** | **3** | **4** | **5** | **6** |
| Guidance documents | AGD_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Life-cycle support | ALC_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 |
| | ALC_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 |
| | ALC_DEL | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | **1** | 1 | 1 | 1 | **2** |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 |
| Security Target evaluation | ASE_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| | ASE_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 |
| | ATE_DPT | | | **1** | 1 | **3** | 3 | **4** |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** |
| Vulnerability assessment | AVA_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 |

- The number in the table denotes the component number included in the EAL package
- If no number is given the family is not contained in the respective EAL package
- E.g. EAL3 contains ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, etc.
- Security Target Evaluation (ASE) and Guidance Documents (AGD) are (almost) always the same
- Vulnerability Assessment (AVA_VAN) appears rather small with just one family, but usually requires the majority of the evaluation effort, especially in higher EALs

see CC Part 3, Annex E


ASE
SFR
Security Target
ATE
AGD
ADV
ALC
AVA
Paper Work
ITSEF
SFR
ATE
ADV
Functional Security
Vulnerability Assessment
ADV
AGD
AVA

# Secure **Product** Lifecycle



# QUESTIONS ?