Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Preparing and Implementing the Cyber Resilience Act in Organizations

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

- Lead Auditor for Management Systems (information security, services, quality, and more).
- Chairman of the **Institute for Artificial Intelligence**.
- Deputy Manager of the **Bulgarian Union of Standardizers**.
- Active participant in numerous European and national cybersecurity projects.
- Assistant Professor at **UniBIT**:
  - Cybersecurity Standards
  - Cybersecurity Management
  - Cryptography
  - Zero Trust Architectures

Focus Points

- **European Commission Guidance for CRA Implementation**
Latest instructions, scope clarifications, and practical expectations for manufacturers, developers, and organizations in the digital product ecosystem.

- **Certification and Conformity Assessment**
Understanding the role of notified bodies, when self-assessment is allowed, and how organizations can demonstrate compliance.

- **Practical Part 1: Organizational Preparation**
Conducting a gap analysis, updating internal policies, and aligning internal processes with CRA requirements.

Focus Points

- **Common Criteria (CC) and EUCC**
  Key differences between the international Common Criteria framework and the EU-focused EUCC scheme; advantages of the European approach for CRA readiness.

- **Practical Part 2: Building a Compliance Roadmap**
  Developing a clear and realistic plan for implementation, responsibilities, timelines, and evidence collection.

- **Conclusion: What We Learned and What Comes Next**
  Summary of the session, expected upcoming steps under CRA, and short presentation of the OSCRAT project.

Q&A

- **How to ask:** Post questions in the **chat window**
- **When answered**
  - End of the current session
  - Beginning of the next session
- **Special cases**
  - Some questions may require deeper research
  - Answers may be provided later via **email**
- **Future opportunities**
  - Dedicated discussion slots in next sessions
  - Interactive Q&A during the workshops

Hot Guidance from the European Commission on Implementing the CRA

An expert briefing on the latest updates and your path forward.

Miroslav Mitev

Based on the European Commission's 'Cyber Resilience Act – Implementation' page, last updated December 3, 2025.

Our Focus for the Next 20 Minutes

The Latest Intelligence: What‘s new in the EC’s December 3, 2025 update.

The Official Blueprint: Exploring the EC’s four implementation ‘pathways’ for Manufacturers, Member States, SMEs, and the Open-Source community.

The Highway to Compliance: Understanding the critical role of standardization and the timeline to 2027.

Your Action Plan: Defining practical steps for your organization in 2026.

The Executive Briefing: What's New as of December 3, 2025

Key Insight: The EC has moved from principles to a structured implementation framework.

A New Central Hub

The EC has launched a structured 'Cyber Resilience Act – Implementation' portal with four distinct entry points:

- Manufacturers
- Member States
- SMEs
- Open-source community

New Legislation Published

Implementing Act (Dec 1, 2025): Provides technical descriptions for 'important' and 'critical' products (Annex III & IV). This reduces ambiguity for high-risk categories.

What's on the Immediate Horizon

- **Delegated Act (Expected Dec 2025):** Will specify rules for CSIRTs and notification delays within the Single Reporting Platform.
- **First EC Guidance Package (Expected Early 2026):** Will provide official interpretations and clarity.

The EC's New Blueprint: Four Doors to Implementation

CRA IMPLEMENTATION PORTAL

1. Manufacturers

Guidance on new obligations: design, documentation, vulnerability management, monitoring, and reporting. (This is your primary entrance).

2. Member States

Role in market surveillance, notifying Conformity Assessment Bodies (CABs), and coordinating with ENISA.

3. SMEs & Startups

Promised support tools, simplified documentation forms, and dedicated funding via the Digital Europe Programme.

4. Open-Source Community

Critical clarification on the distinction between non-commercial projects and commercial products using open-source components.

These portals are the EC's direct signal on how they expect different groups to organize their preparation. It's our clearest look yet into their operational thinking.

A Manufacturer’s Obligations: From Design to Post-Market

Before Placing on the Market

- Conduct a comprehensive **risk assessment**.
- Implement essential cybersecurity requirements, using **harmonised standards** to guide the process.
- Prepare detailed **technical documentation**.
- Perform a **conformity assessment** procedure (details on the next slide).

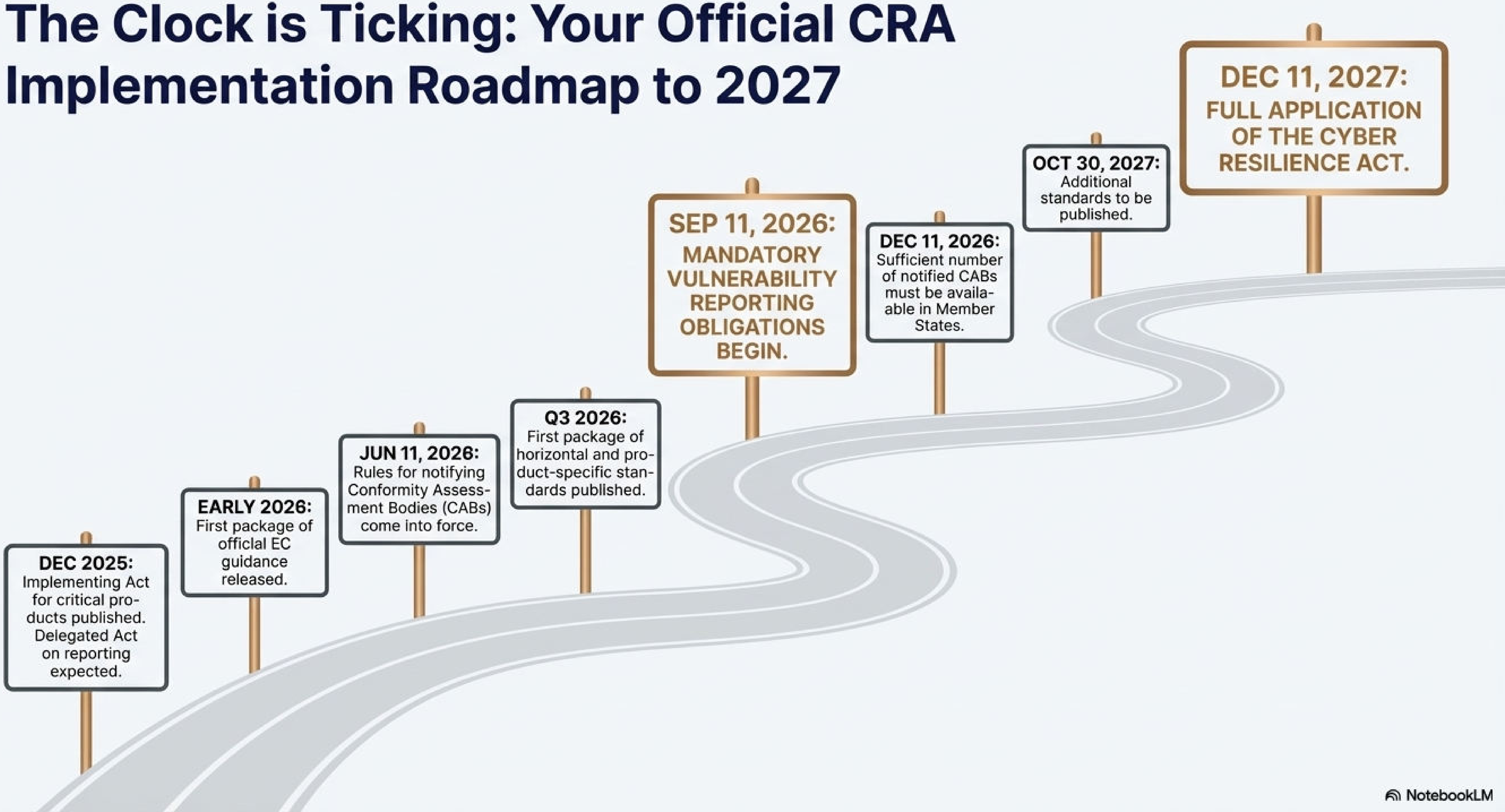
At Placement on the Market

- Affix the **CE marking** to the product.
- Attach a signed **declaration of conformity**.
- Clearly state the **support period** for the product.
- Provide clear **information and instructions** to the user.

After Placement on the Market

- Actively **handle vulnerabilities** for the entire support period.
- **Report** actively exploited vulnerabilities and severe incidents to authorities.

The Clock is Ticking: Your Official CRA Implementation Roadmap to 2027



DEC 2025: Implementing Act for critical products published. Delegated Act on reporting expected.

EARLY 2026: First package of official EC guidance released.

JUN 11, 2026: Rules for notifying Conformity Assessment Bodies (CABs) come into force.

Q3 2026: First package of horizontal and product-specific standards publlshed.

SEP 11, 2026: MANDATORY VULNERABILITY REPORTING OBLIGATIONS BEGIN.

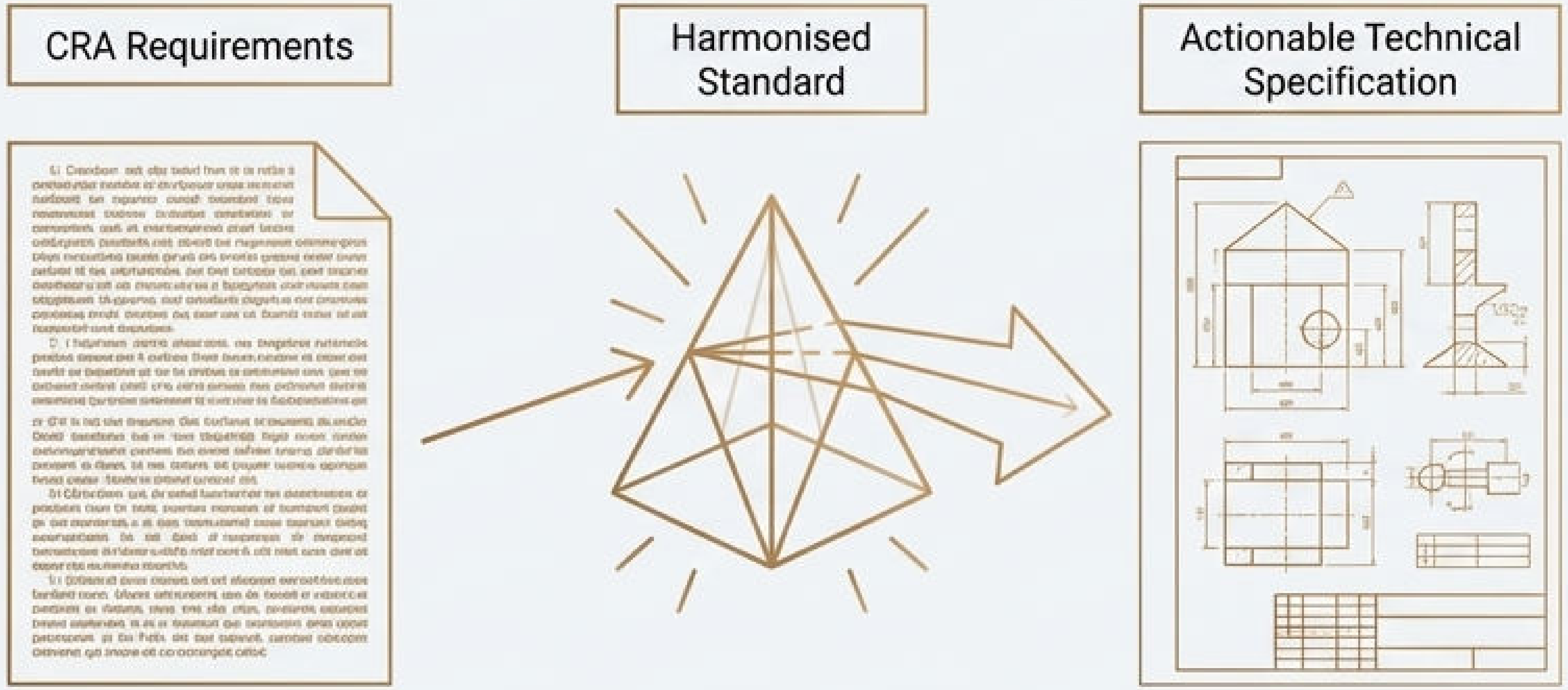
DEC 11, 2026: Sufficient number of notified CABs must be available in Member States.

OCT 30, 2027: Additional standards to be published.

DEC 11, 2027: FULL APPLICATION OF THE CYBER RESILIENCE ACT.

Standardization: The Highway to Presumption of Conformity

Core Concept: Products in conformity with **harmonised standards** benefit from a **presumption of conformity** with the CRA’s essential requirements.



CRA Requirements

Harmonised Standard

Actionable Technical Specification

- Harmonised standards “translate” legal obligations into actionable technical specifications.
- The process is led by European Standardisation Organisations (ESOs) in close cooperation with industry.
- The EC requires balanced participation, specifically calling out the need for involvement from consumer organizations and the open-source community.

Practical Takeaway: For manufacturers, this means the CRA is not just a set of abstract rules from Brussels, but a concrete set of standards you can directly implement in your processes.

Decoding Standardisation Request M/606: The Framework Takes Shape

41

standards are included in the request to support the CRA

Breakdown of Standards

- **Horizontal Standards**: Provide common frameworks and processes applicable to all products (e.g., vulnerability management, secure development).
- **Vertical (Product-Specific) Standards**: Provide tailored specifications for specific product types, with the first package prioritising "Important" and "Critical" products (Annex III & IV).

Additional Deliverables from ESOs

- **Common Terminology**
- **Sectoral Risk Assessment Methodologies**
- **A Common Threat Catalogue**

Key Implication: This structured approach provides a clear path for integrating security into the product lifecycle.

How to Engage: Shape the Standards You Will Be Judged Against

The EC highlights two key platforms for engagement:

STAN4CR (‘CRA European standards’)

The official portal where ESOs publish all information and updates on the development of CRA standards.

CYBERSTAND.eu

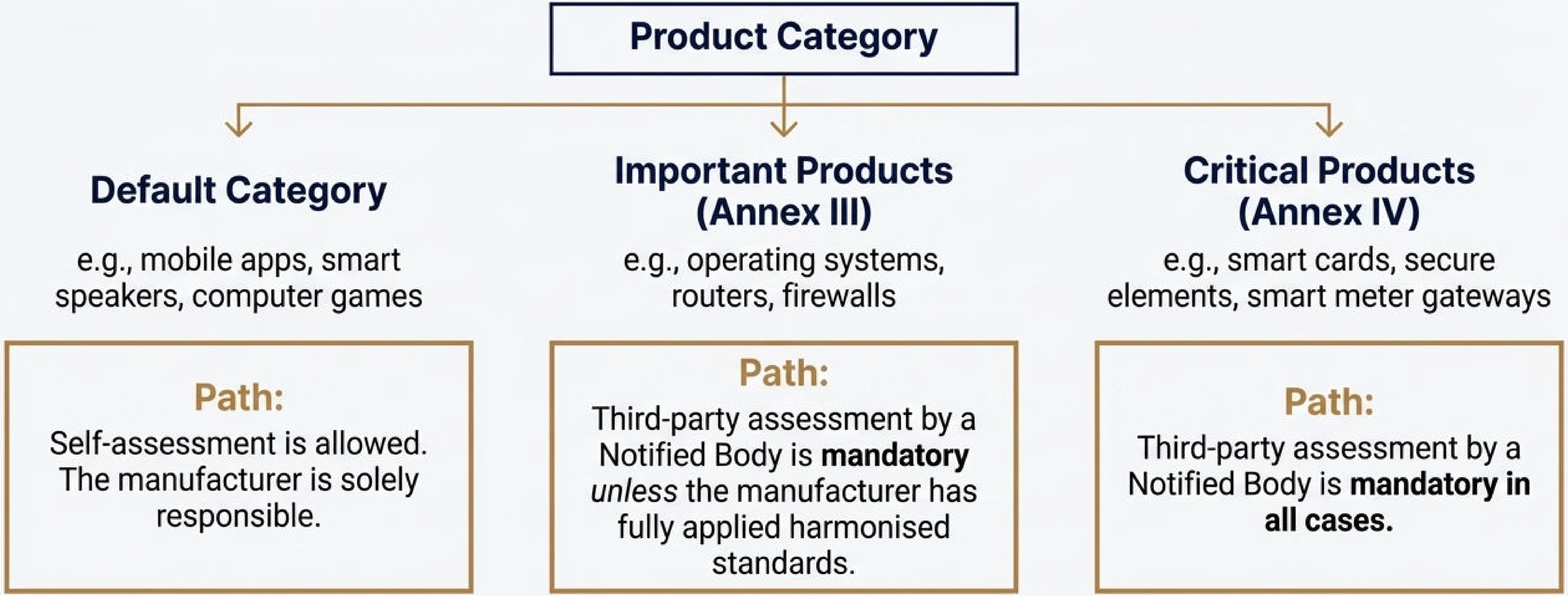
An initiative to encourage and empower European stakeholders to actively participate in developing standards and conformity schemes.

Is your organization participating in technical committees or national mirror committees?

These standards will define the future of your:

- Technical documentation requirements.
- Vulnerability management procedures.
- Product testing and assessment protocols.

Navigating Conformity Assessment: Self-Assessment vs. Notified Bodies



Product Category

Default Category

e.g., mobile apps, smart speakers, computer games

Path:

Self-assessment is allowed. The manufacturer is solely responsible.

Important Products (Annex III)

e.g., operating systems, routers, firewalls

Path:

Third-party assessment by a Notified Body is **mandatory** *unless* the manufacturer has fully applied harmonised standards.

Critical Products (Annex IV)

e.g., smart cards, secure elements, smart meter gateways

Path:

Third-party assessment by a Notified Body is **mandatory in all cases.**

The technical descriptions for these product categories are now specified in **Implementing Regulation (EU) 2025/2392.** Notified Bodies will be listed on the EC's NANDO website.

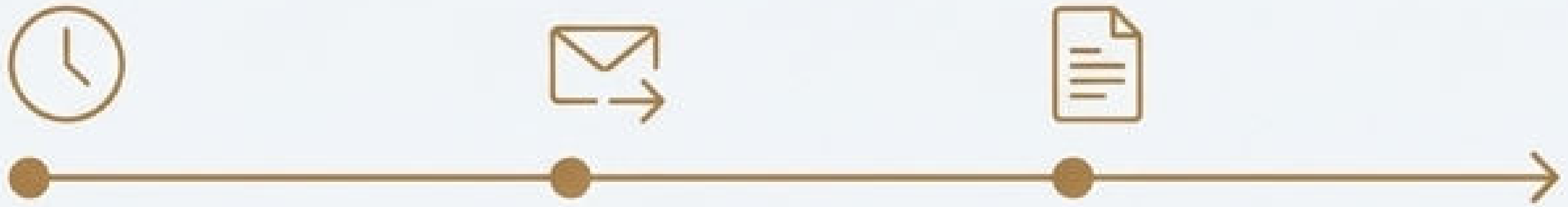
The New Reporting Mandate: 24 Hours to Respond

Effective Date: **September 11, 2026**

The Rule

Manufacturers must report **actively exploited vulnerabilities** and **severe incidents** impacting product security.

The Reporting Timeline



< 24 Hours
(from awareness)

Submit an early warning.

< 72 Hours

Submit a full notification.

< 14 Days
(after fix is available)

Submit a final report for exploited vulnerabilities.

The Process

Manufacturers report **once** via the **CRA Single Reporting Platform (SRP),** currently being built by ENISA.

The notification goes to the national CSIRT, which shares it with ENISA and other relevant CSIRTs.

A Delegated Act will specify grounds for CSIRTs to delay dissemination in exceptional cases.

Your Minimum Viable Compliance Roadmap for 2026

1. Classify Your Portfolio

- Identify every product in scope of the CRA.
- Determine which fall into the 'important' and 'critical' categories based on the new Implementing Act.

2. Conduct a Gap Analysis

- Benchmark your current secure development and vulnerability management practices against the CRA's essential requirements.
- Map against forthcoming harmonised standards as they are published.

3. Prepare Your Documentation

- Begin updating technical descriptions, user manuals, and security information.
- Formalize your vulnerability handling and reporting processes to meet the 24/72h deadlines.

4. Coordinate and Monitor

- Align CRA efforts with other compliance regimes (NIS2, GDPR, ISO/IEC 27001, etc.).
- Closely monitor the EC's guidance and the ESOs' standardization progress throughout the year.

Your Essential CRA Toolkit: Authoritative Resources & Community Hubs

Official EC Pages

- **Main Portal**: "Cyber Resilience Act – Implementation"
- **Stakeholder Pages**: Links to the specific sub-pages for Manufacturers, Member States, SMEs, and Open-source.
- **Standardisation Hub**: "Cyber Resilience Act – Standardisation" (Details on M/606, STAN4CR, CYBERSTAND.eu).

Key Documents

- **FAQ – Cyber Resilience Act implementation**: The EC's official Q&A covering scope, open-source, and relation to other regulations.

Community & Updates

- **CRA Community Subscription**: Link to sign up for official email updates from the Commission.

Three Core Messages from the EC's Latest Guidance

The Era of Ambiguity is Over.

The CRA now has a clear, date-driven roadmap to full implementation on December 11, 2027. The window for preparation is defined and finite.

Standards Are Not Optional; They Are the Mechanism.

Harmonised standards are the primary tool for demonstrating compliance. Engaging with their development is a strategic necessity, not an academic exercise.

Proactive Integration Beats Last-Minute Reaction.

Organizations that start now can methodically integrate CRA requirements into their DevSecOps, governance, and product lifecycle processes. Those who wait will face a chaotic and costly reaction in 2027.

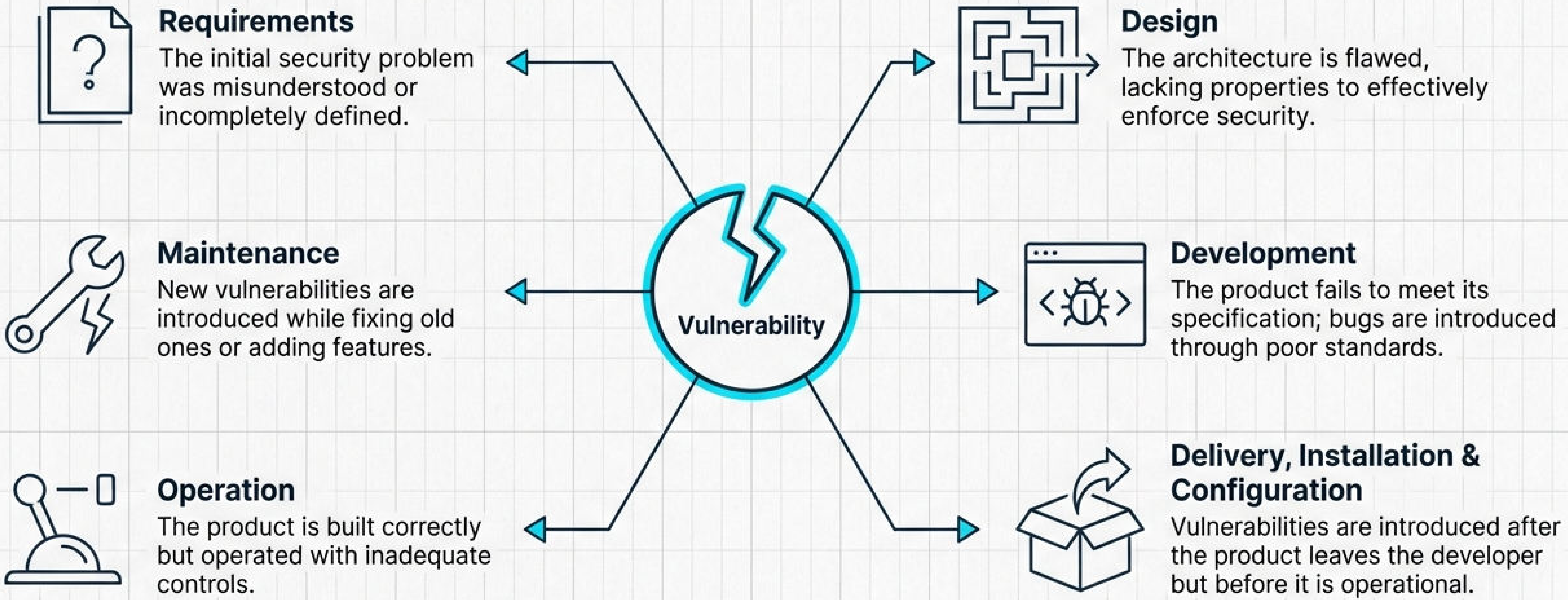
Engineering Trust: A Blueprint for ISO/IEC 15408-3 Security Assurance

A Structured Guide to the Common Criteria’s Assurance Components

This presentation deconstructs the framework used to build and verify trust in IT products, transforming the dense ISO standard into an actionable mental model.

The Genesis of Vulnerability

The Common Criteria assurance framework exists to counter a fundamental problem: IT security breaches arise from the intentional exploitation or unintentional triggering of vulnerabilities. These vulnerabilities are not random; they stem from specific failures across the product lifecycle.



Requirements
The initial security problem was misunderstood or incompletely defined.

Design
The architecture is flawed, lacking properties to effectively enforce security.

Maintenance
New vulnerabilities are introduced while fixing old ones or adding features.

Development
The product fails to meet its specification; bugs are introduced through poor standards.

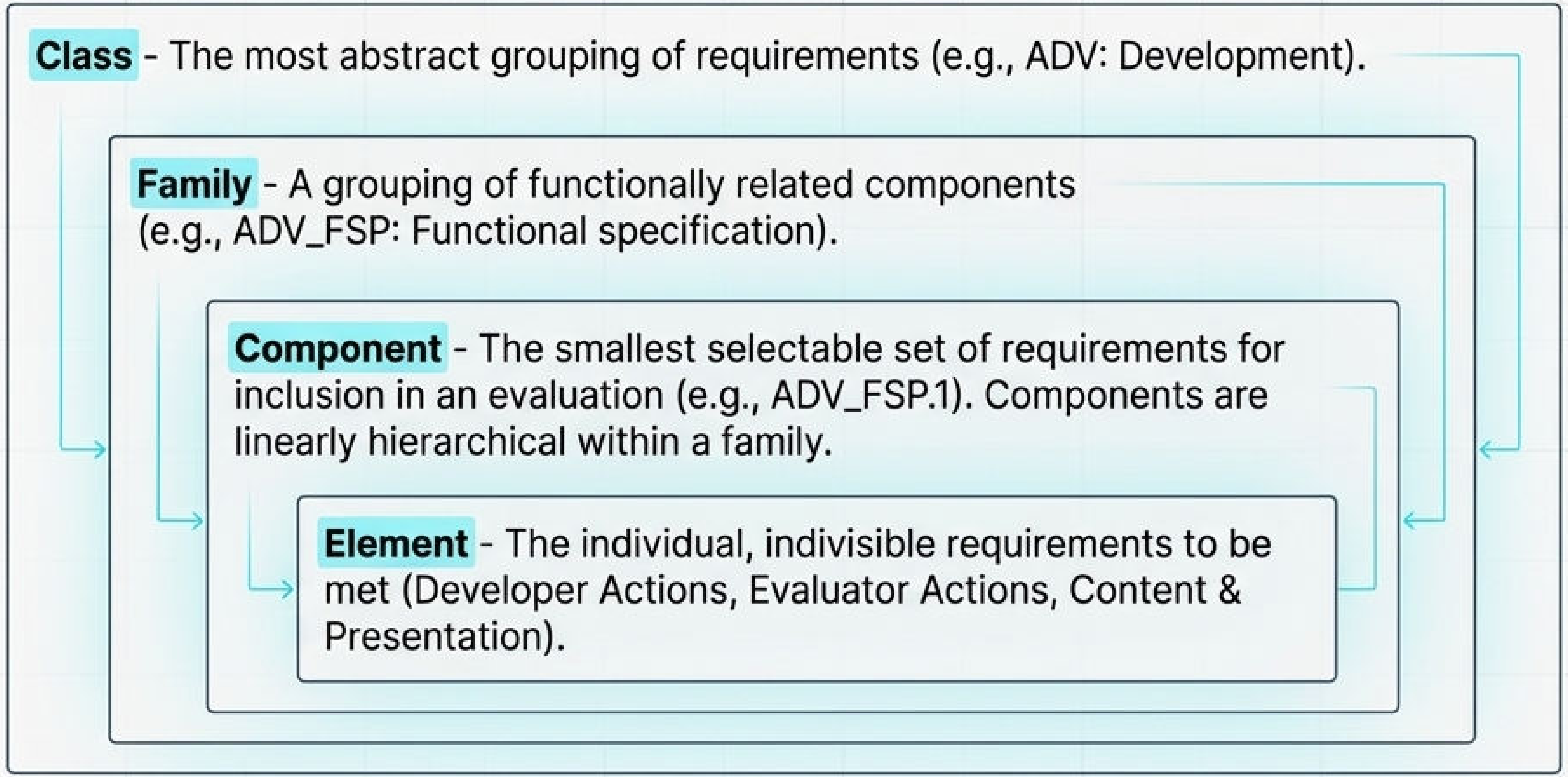
Operation
The product is built correctly but operated with inadequate controls.

Delivery, Installation & Configuration
Vulnerabilities are introduced after the product leaves the developer but before it is operational.

Based on ISO/IEC 15408-3

The Common Criteria Approach: Assurance Through Evaluation

The ISO/IEC 15408 series provides assurance through **active investigation**—a structured evaluation of an IT product by expert evaluators, with increasing emphasis on scope, depth, and rigour.



Class - The most abstract grouping of requirements (e.g., ADV: Development).

Family - A grouping of functionally related components (e.g., ADV_FSP: Functional specification).

Component - The smallest selectable set of requirements for inclusion in an evaluation (e.g., ADV_FSP.1). Components are linearly hierarchical within a family.

Element - The individual, indivisible requirements to be met (Developer Actions, Evaluator Actions, Content & Presentation).

ISO/IEC 15408-3

Defines the *Security Assurance Requirements* (SARs) – the '**what**' to prove.

ISO/IEC 18045

Defines the *Methodology for IT Security Evaluation* – the '**how**' to prove it.

ISO/IEC 15408-3:2022, 6.2-6.5

The Assurance Landscape: A Thematic Framework

Defining the Blueprint (Specification & Definition)

APE: Protection Profile (PP) evaluation

ACE: Protection Profile Configuration evaluation

ASE: Security Target (ST) evaluation

Pillar objective:
Establishing a clear, consistent, and correct definition of the security problem, objectives, and requirements.

Building with Integrity (Development & Lifecycle)

ADV: Development

AGD: Guidance documents

ALC: Life-cycle support

Pillar objective:
Ensuring the product is constructed and maintained using disciplined, secure, and verifiable processes.

Proving Resilience (Verification & Validation)

ATE: Tests

AVA: Vulnerability assessment

Pillar objective:
Demonstrating that the finished product functions as specified and resists attacks from credible threats.

Assembling with Confidence (Composition)

ACO: Composition

Pillar objective:
Providing assurance for products built by integrating previously evaluated components.

Part 1: The Blueprint – Defining the Scope

Before a product can be judged secure, we must have an unambiguous, internally consistent, and sound specification of the security problem it solves. The APE, ACE, and ASE classes provide the assurance requirements for these foundational documents.

Protection Profile (PP) - Class APE

A reusable, implementation-independent statement of security needs for a *class* of products (e.g., a firewall, a smart card). It defines a security problem common to that technology type.

PP-Configuration - Class ACE

A modern, modular construct allowing the combination of PPs and smaller "PP-Modules" to define requirements for more complex products. Essential for component-based systems.

Security Target (ST) - Class ASE

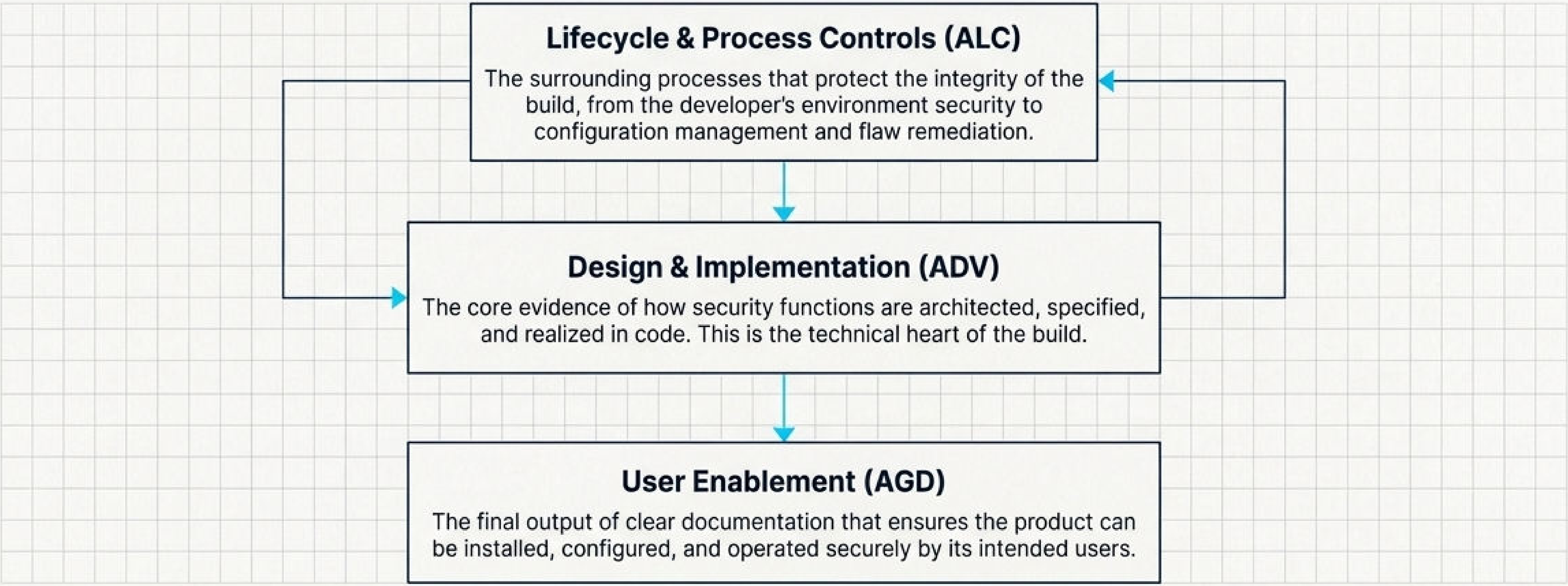
The security specification for a *single, specific* product—the Target of Evaluation (TOE). It states the security requirements and makes a precise claim of conformance to one or more PPs.

KEY TAKEAWAY

The ST is the ultimate blueprint for a specific TOE evaluation. PPs and PP-Configurations provide the standardized, reusable templates from which STs are often built.

Part 2: The Build – Building with Integrity

Assurance is not just about the final product; it's about the integrity of the entire process used to create it. These classes provide evidence that the TOE was developed, documented, and is supported in a way that minimizes the introduction of vulnerabilities.



Lifecycle & Process Controls (ALC)

The surrounding processes that protect the integrity of the build, from the developer's environment security to configuration management and flaw remediation.

Design & Implementation (ADV)

The core evidence of how security functions are architected, specified, and realized in code. This is the technical heart of the build.

User Enablement (AGD)

The final output of clear documentation that ensures the product can be installed, configured, and operated securely by its intended users.

"Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development, production, delivery and maintenance activities."

ADV: The Development Dossier

To provide a transparent and traceable path from high-level security functions down to the implementation, proving the design is sound and the TOE cannot be easily corrupted or bypassed.

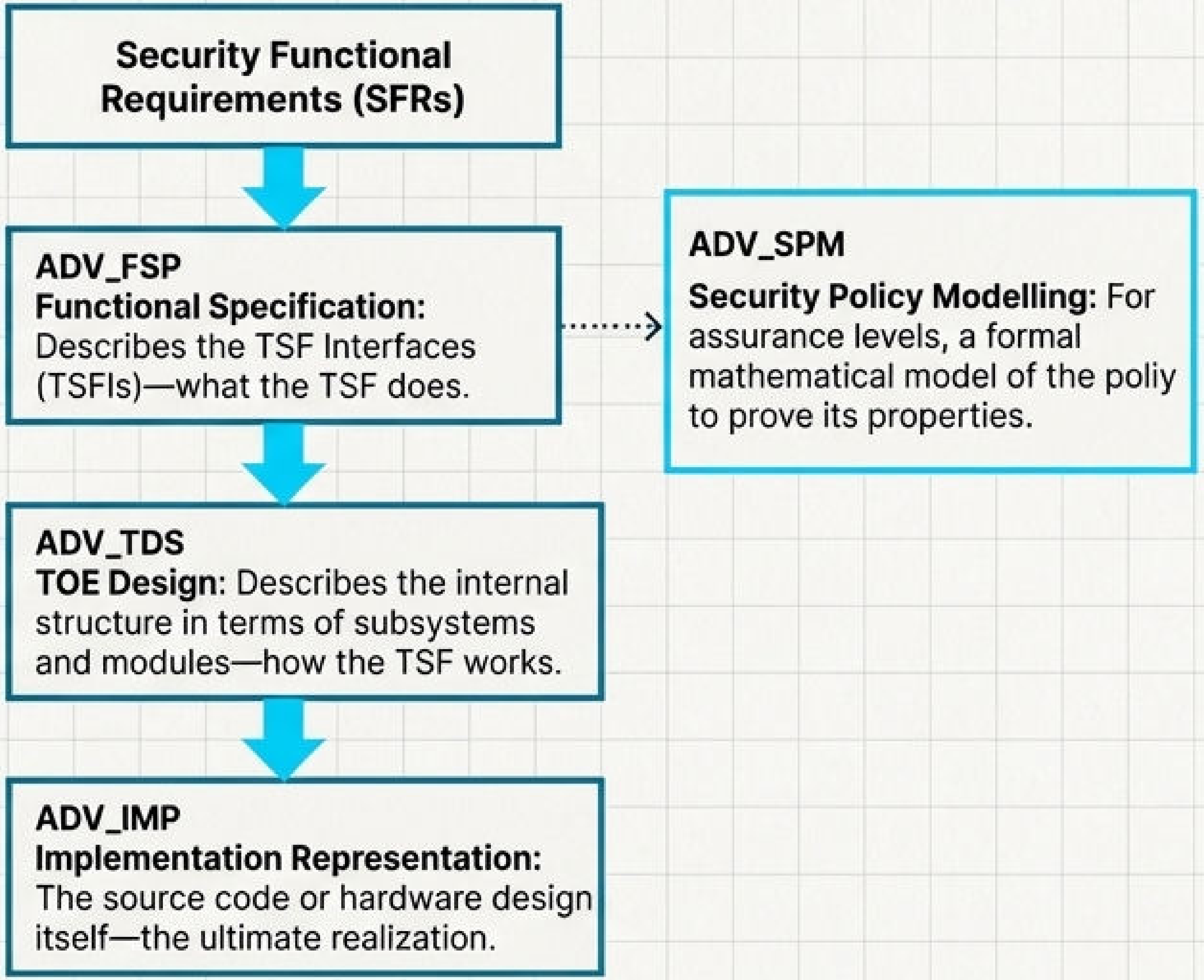
ADV_ARC Security Architecture

Describes core protective properties:

Self-protection: The TSF protects itself from tampering.

Domain separation: The TSF keeps untrusted entities isolated from each other.

Non-bypassability: TSF security functions are always invoked and cannot be circumvented.



Security Functional Requirements (SFRs)

ADV_FSP
Functional Specification: Describes the TSF Interfaces (TSFIs)—what the TSF does.

ADV_SPM
Security Policy Modelling: For assurance levels, a formal mathematical model of the poliy to prove its properties.

ADV_TDS
TOE Design: Describes the internal structure in terms of subsystems and modules—how the TSF works.

ADV_IMP
Implementation Representation: The source code or hardware design itself—the ultimate realization.

Supporting the Build: Lifecycle Controls and User Guidance

ALC: Life-cycle Support

Objective: To establish security controls in the development, production, delivery, and maintenance of the TOE.

Key Families & Purpose

- ALC_CMC **(CM Capabilities) &** ALC_CMS **(CM Scope):** Ensures integrity of configuration items via a robust Configuration Management system. Prevents unauthorized changes.
- ALC_DVS **(Developer Environment Security):** Protects the confidentiality and integrity of the TOE design in its development environment (physical, logical, procedural controls).
- ALC_FLR **(Flaw Remediation):** Mandates a process for tracking, correcting, and distributing fixes for security flaws discovered post-release.
- ALC_DEL **(Delivery):** Defines secure procedures to distribute the TOE to the consumer, preventing tampering or counterfeiting.

AGD: Guidance Documents

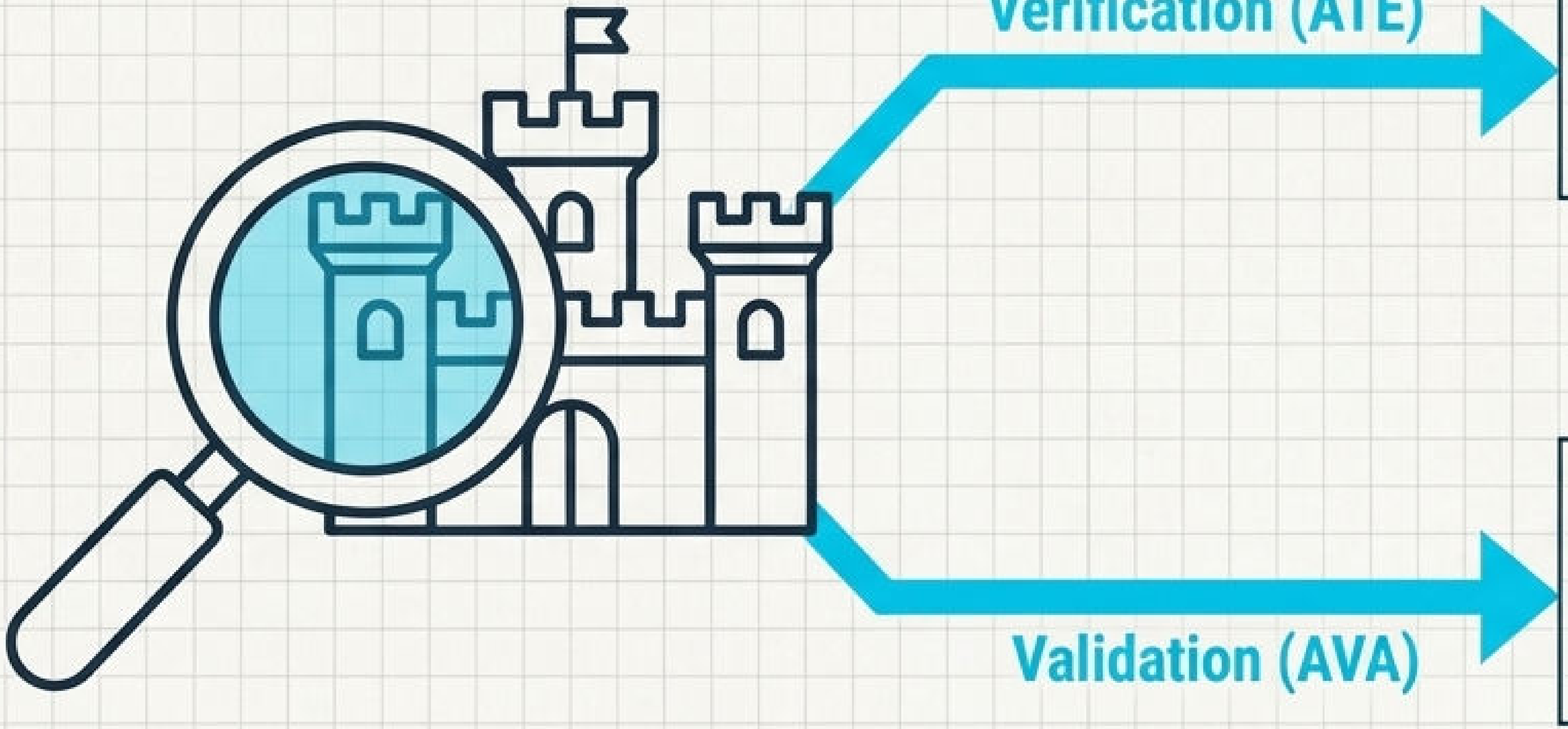
Objective: To minimize the risk of human error in operation that could result in an undetected insecure state.

Key Families & Purpose

- AGD_PRE **(Preparative Procedures):** Describes all steps for secure acceptance and installation of the TOE, transforming it into its evaluated configuration.
- AGD_OPE **(Operational User Guidance):** Describes user-accessible functions, security parameters, and secure procedures for all modes of operation for each user role (e.g., end-user, administrator).

Part 3: The Inspection – Proving Resilience

A secure design and build process are necessary **but not sufficient**. Assurance requires rigorous, independent verification that the final product behaves as specified and is resistant to expert attacks.



‘Does it do what the blueprint says?” → Leads to confirmation of correct behavior.

“Can its defenses be breached?” → Leads to confidence in its strength.

Testing in **ATE** provides assurance that the TSF behaves as described in the ADV evidence. **Vulnerability Assessment** in **AVA** actively searches for weaknesses an attacker could exploit, regardless of the specification.

NotebookLM

Verification (ATE) and Validation (AVA)

ATE: Tests

"To provide assurance that the TSF behaves as described."

Key Families & Activities

- **ATE_FUN** Functional Tests: Developer-conducted tests showing the product meets its functional requirements.
- **ATE_COV** Coverage: Analysis demonstrating that the tests cover the TSF interfaces (ADV_FSP).
- **ATE_DPT** Depth: Analysis demonstrating that the tests exercise the internal TSF subsystems and modules (ADV_TDS).
- **ATE_IND** Independent Testing: Evaluator-conducted testing, including repeating a sample of developer tests and devising new ones to confirm the TSF operates as specified.

AVA: Vulnerability Assessment

A systematic search for flaws that would allow an attacker to violate the security policy.

Core Family

- **AVA_VAN** Vulnerability Analysis, which is leveled based on attacker capability.

Evaluator Actions

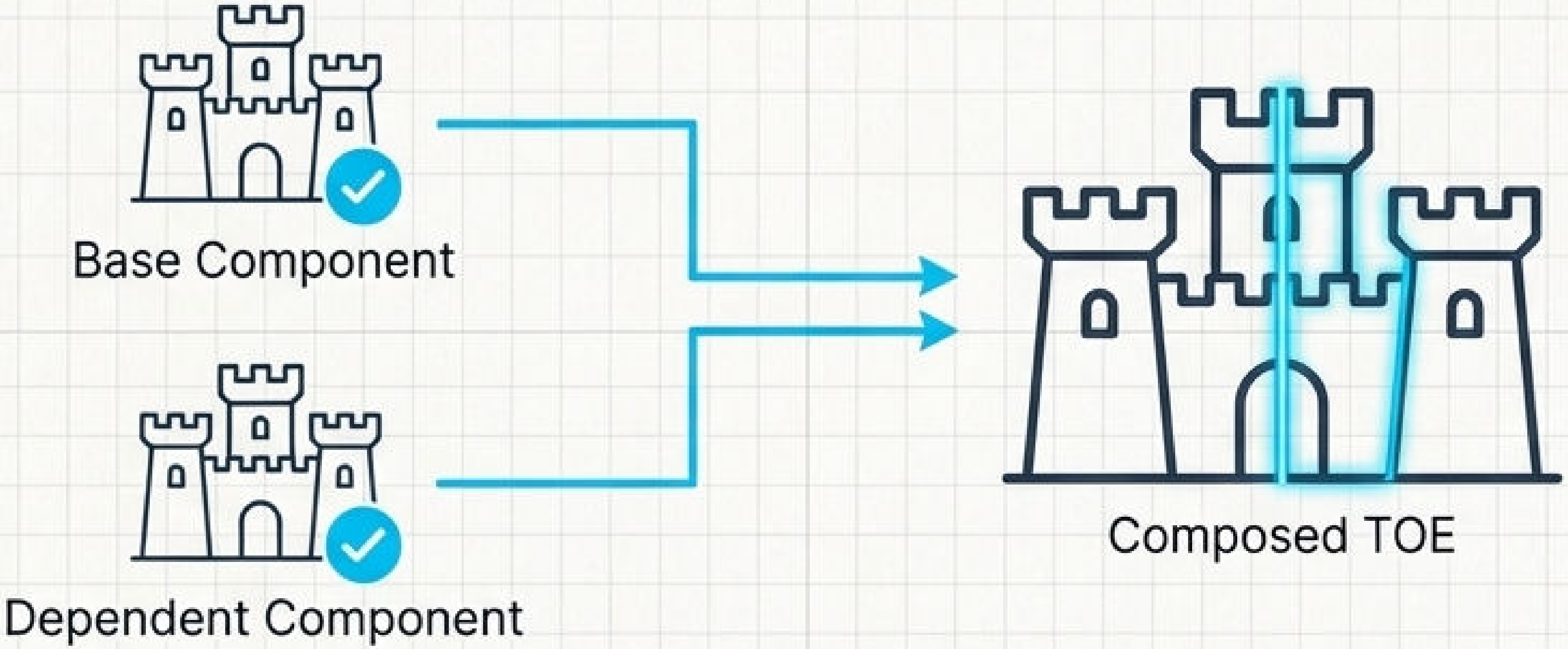
- Conduct a search of public domain vulnerability information.
- Perform an independent vulnerability analysis of the design (ADV) and guidance (AGD) to hypothesize flaws.
- Conduct penetration testing to confirm the TOE is resistant to attacks up to a specified 'Attack Potential.'

Key Concept

Attack Potential (from ISO 18045) is a calculated measure based on attacker expertise, knowledge, time, and equipment. Higher AVA_VAN levels require resistance to higher attack potentials.

A Special Case: Assembling Pre-Built Fortresses

Re-evaluating an entire system from scratch every time a pre-certified component is integrated is inefficient. The ACO class provides a dedicated assurance method for building a *composed TOE* from previously evaluated base and dependent components.



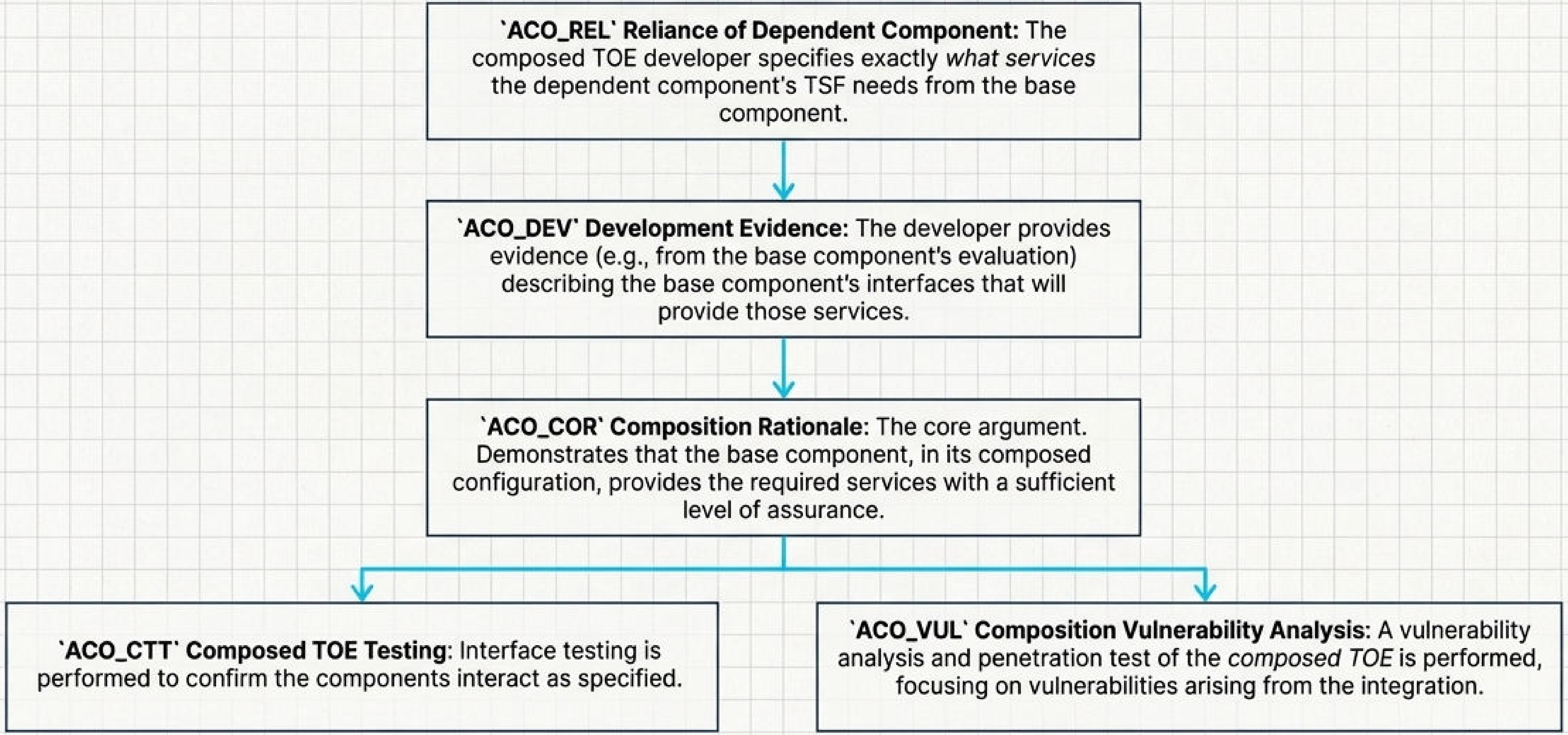
"[ACO provides] a method...to gain confidence in a TOE that is the combination of two or more successfully evaluated components without having to re-evaluate the composite TSF." - ISO/IEC 15408-3:2022, 15.1

How do we trust the *seams*?

The focus of ACO is ensuring the components interact securely in their new, combined configuration.

ACO: The Assurance of Composition

To demonstrate that the base component provides appropriate, assured support for the dependent component, and that their integration introduces no new vulnerabilities.



`ACO_REL` Reliance of Dependent Component: The composed TOE developer specifies exactly *what services* the dependent component's TSF needs from the base component.

`ACO_DEV` Development Evidence: The developer provides evidence (e.g., from the base component's evaluation) describing the base component's interfaces that will provide those services.

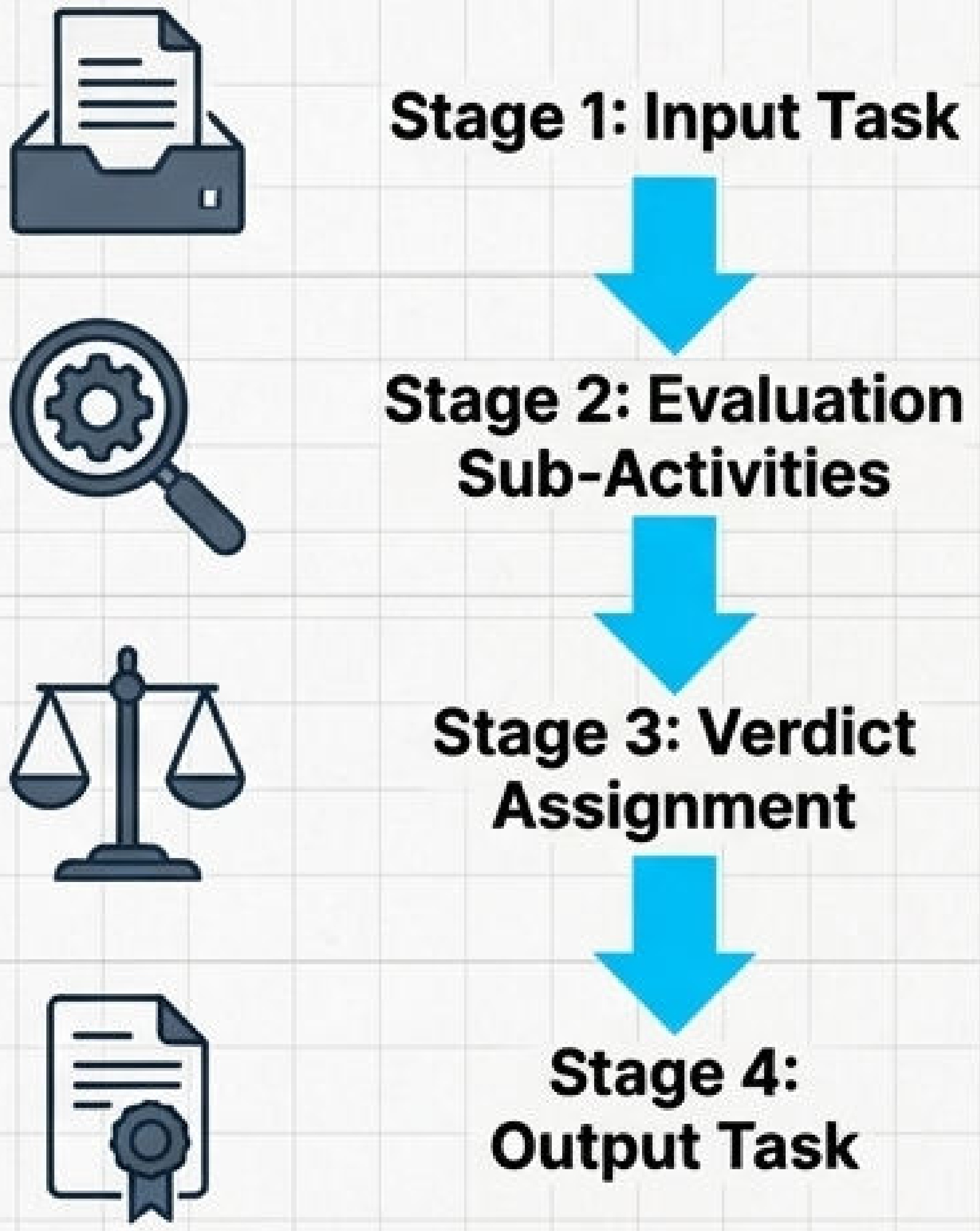
`ACO_COR` Composition Rationale: The core argument. Demonstrates that the base component, in its composed configuration, provides the required services with a sufficient level of assurance.

`ACO_CTT` Composed TOE Testing: Interface testing is performed to confirm the components interact as specified.

`ACO_VUL` Composition Vulnerability Analysis: A vulnerability analysis and penetration test of the *composed TOE* is performed, focusing on vulnerabilities arising from the integration.

From Requirements to Verdict: The Evaluator’s Process

Core Idea: Assurance requirements are not self-enforcing. An accredited evaluator uses the methodology in **ISO/IEC 18045** to systematically verify the developer's evidence against each required element in ISO/IEC 15408-3.



Stage 1: Input Task

Evaluator receives the ST and all developer evidence (the ADV, ALC, AGD documentation, etc.).

Stage 2: Evaluation Sub-Activities

For each assurance component (e.g., `ADV_ARC.1`), the evaluator executes a series of prescribed **work units**.

A **Work Unit** is a mandatory, atomic action the evaluator ***shall*** perform (e.g., "The evaluator *shall check* that the security architecture description describes...").

Stage 3: Verdict Assignment

Based on the results of the work units for an evaluator action element, a verdict is assigned.

PASS **PASS**: Requirements are met; evidence is coherent and consistent.

FAIL **FAIL**: Requirements are not met, or evidence is incoherent/inconsistent.

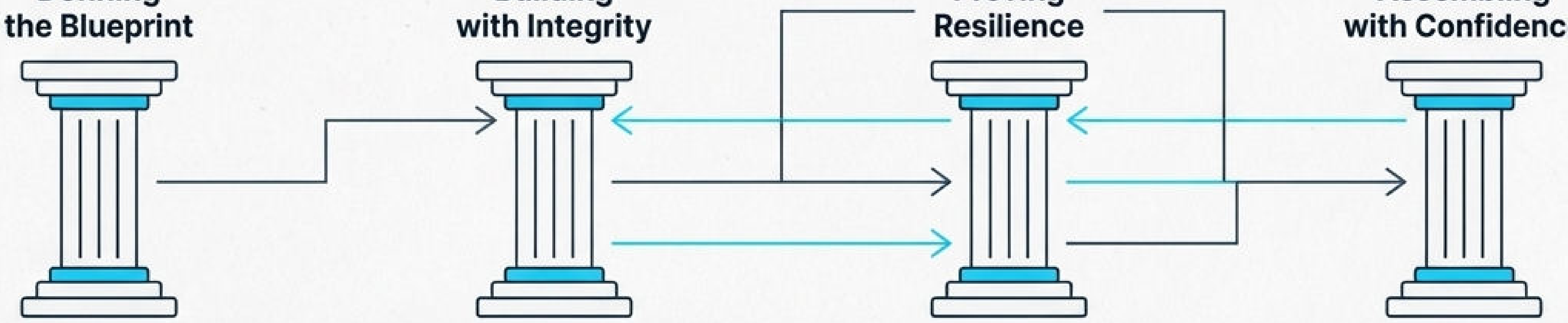
Stage 4: Output Task

The evaluator produces an **Evaluation Technical Report (ETR)**, which provides the technical justification for all verdicts. This ETR is the basis for certification.

Key Insight: This rigorous, repeatable process ensures that a Common Criteria certificate represents a consistent and verifiable level of scrutiny.

The Discipline of Engineering Trust

ISO/IEC 15408-3 does not present a checklist, but a comprehensive, interconnected discipline for engineering and demonstrating trust in an IT product. **It provides a structured argument** that a product is secure because...



Defining the Blueprint

...its security problem and solution are **precisely defined and internally consistent** (APE, ACE, ASE).

Building with Integrity

...it was **constructed using secure, well-documented, and repeatable processes** (ADV, AGD, ALC).

Proving Resilience

...it has been **rigorously tested and proven resistant to skilled attackers** (ATE, AVA).

Assembling with Confidence

...if built from components, their **integration has been explicitly assured** (ACO).

This structured argument is the foundation of verifiable security assurance.

Core Standards and Authorities

Key ISO/IEC Standards

ISO/IEC 15408-3:2022: Security assurance components. (The "What")

ISO/IEC 18045:2022: Methodology for IT security evaluation. (The "How")

ISO/IEC 15408-1:2022: Introduction and general model.

ISO/IEC 15408-2:2022: Security functional components.

Navigating the Structure

Class: Broadest category of assurance (e.g., `ALC`).

Family: Group of related components (e.g., `ALC_CMC`).

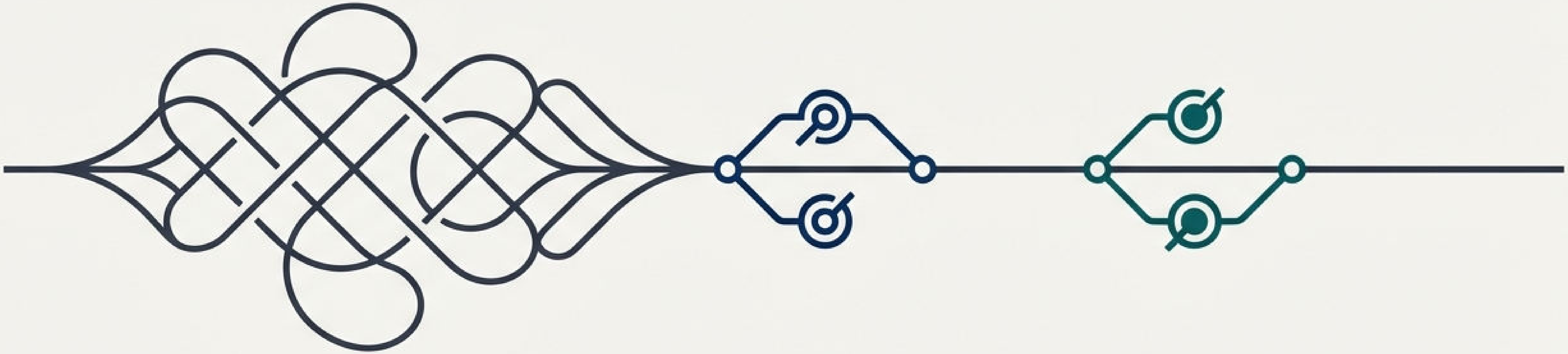
Component: Selectable, leveled requirement set (e.g., `ALC_CMC.4`).

Element: Specific developer/evaluator action or evidence requirement (e.g., `ALC_CMC.4.1D`).

Common Criteria Recognition Arrangement (CCRA)

Purpose: A global arrangement to ensure that certificates issued by one member country are recognized by all others.

List of Certificate Authorizing Members:
- Australia: Australian Signals Directorate
- Canada: Communications Security Establishment
- France: ANSSI
- Germany: BSI
- Japan: IPA
- Netherlands: NLNCSA
- and others



Navigating the Cyber Resilience Act

A Practical Guide to Conformity Assessment

The Cyber Resilience Act (CRA) establishes a new benchmark for cybersecurity in digital products. This guide explains the two essential pathways to demonstrate compliance: third-party certification and manufacturer self-assessment. Understanding these mechanisms is key to ensuring trust, transparency, and security in the European market.

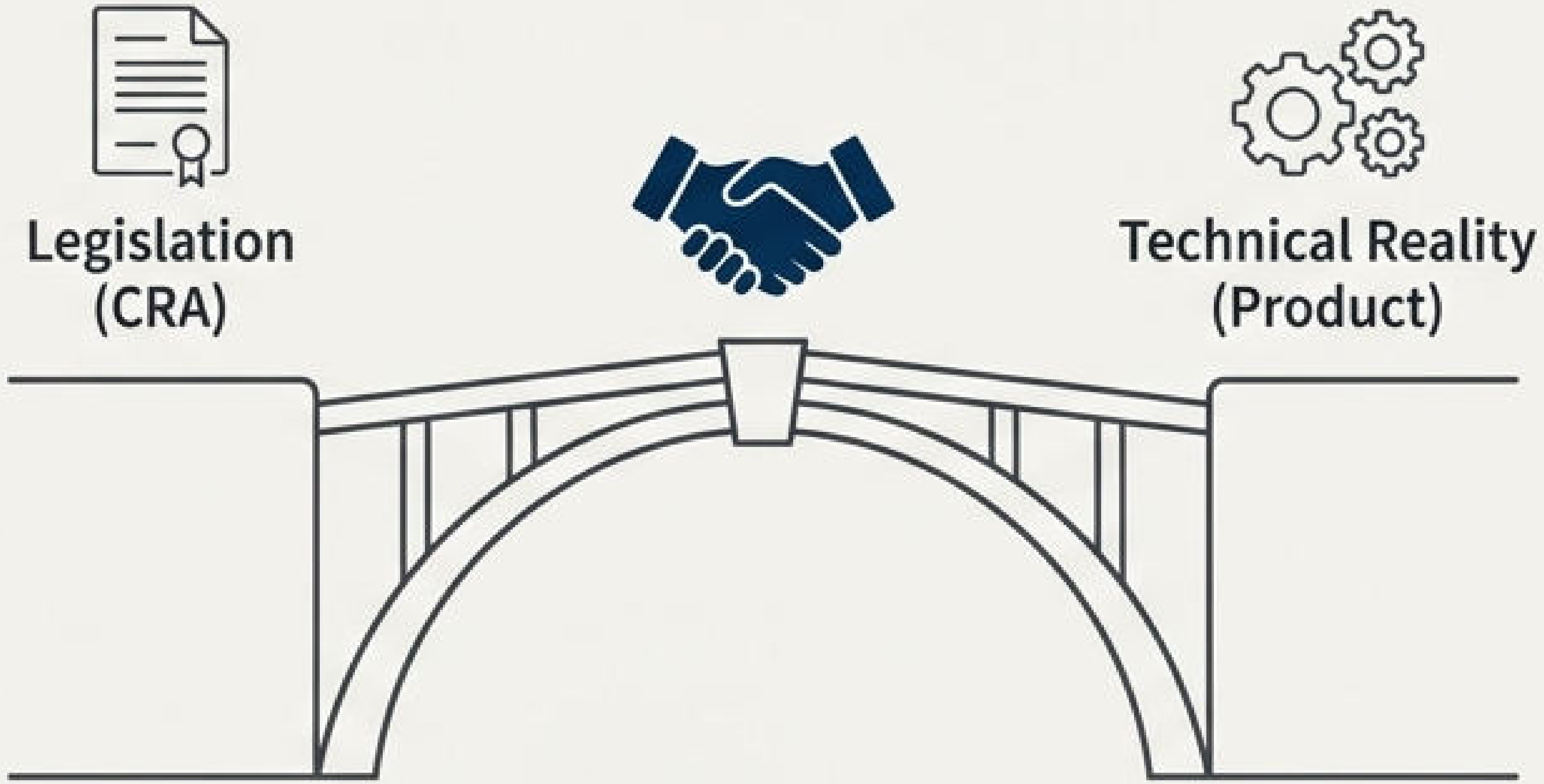
Conformity Assessment is the Bridge Between Legislation and Reality

Conformity assessment is the process of verifying that a product meets specific legal and technical requirements.

Under the CRA, this means proving a product meets the regulation's essential cybersecurity requirements.

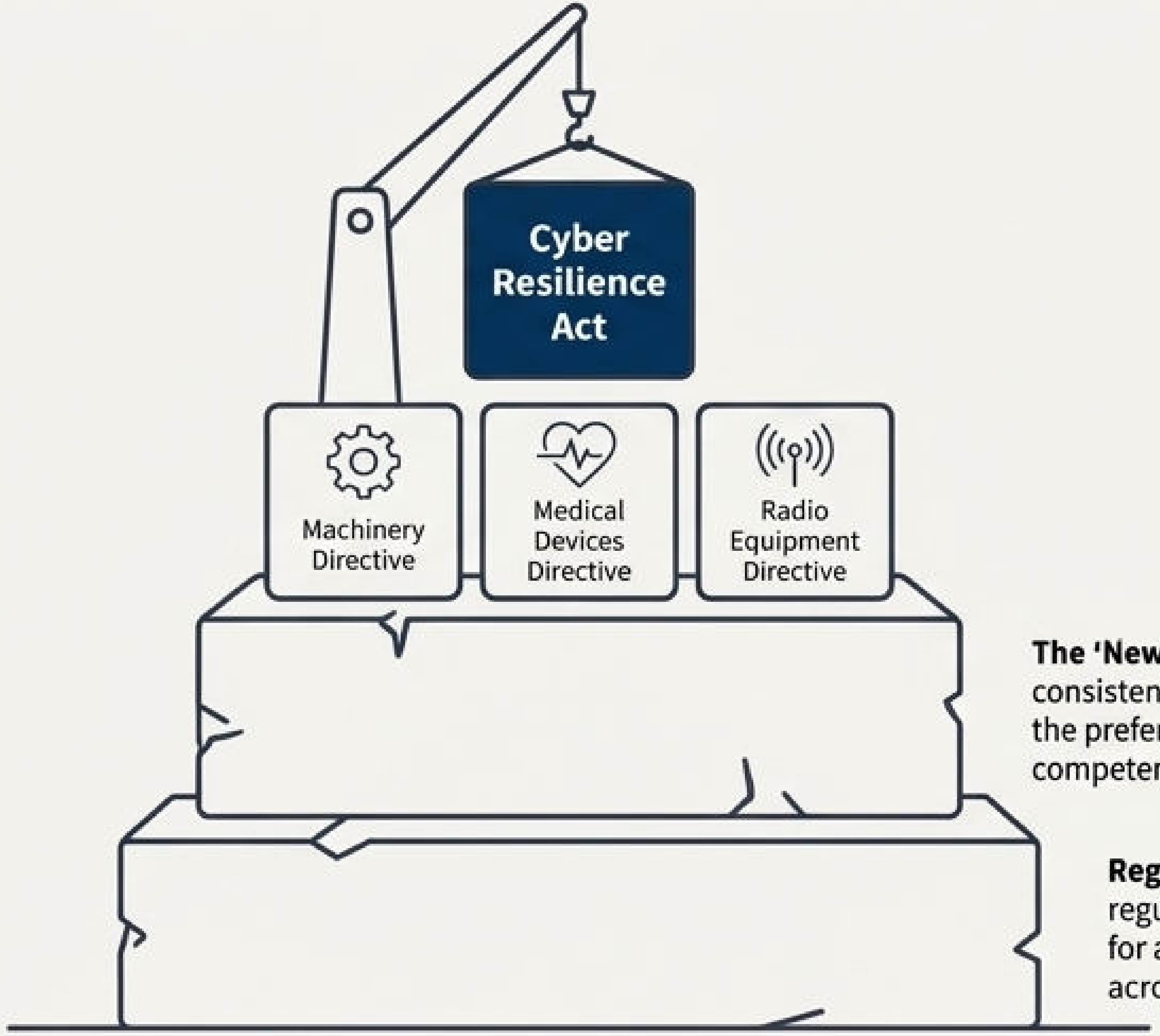
The process can include a combination of testing, auditing, inspection, or certification.

Ultimately, it builds **trust** between manufacturers, regulators, and users.



The CRA's Approach is Built on a Proven EU Framework

The conformity assessment model used in the CRA is not new. It is part of a harmonized system for product safety and quality that has governed the EU market for over a decade.



The 'New Legislative Framework': it created a consistent and reliable system, making accreditation the preferred means to demonstrate the technical competence of conformity assessment bodies.

Regulation (EC) No 765/2008: This regulation established the overall framework for accreditation and market surveillance across the EU.

Two Paths to Compliance, Determined by Product Risk

Third-Party Evaluation

Performed by an independent and accredited **Notified Body**. Mandatory for high-risk or critical products to provide the highest level of assurance.

Self-Assessment

Conducted internally by the manufacturer, who takes full legal responsibility. Permitted for lower-risk products where harmonized standards apply.

Path 1: Understanding Notified Bodies

A Notified Body is an independent organization authorized by an EU Member State and registered with the European Commission to perform conformity assessment for specific product categories. They act as **neutral experts** in cybersecurity assurance.

Accredited Competence

They must be accredited by their their national accreditation body, demonstrating technical competence and independence.

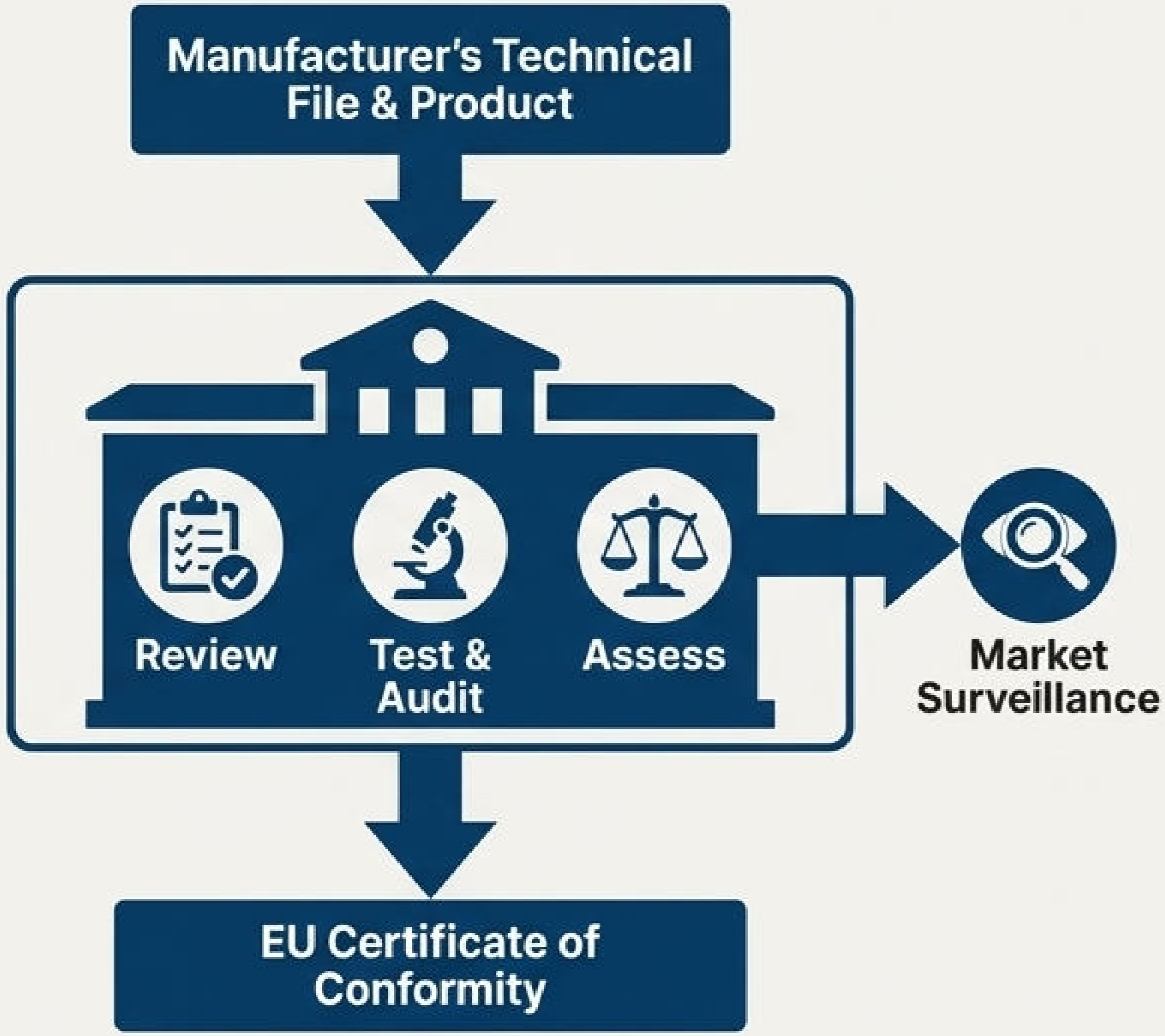
Harmonized Standards

They operate under strict international standards, such as **ISO/IEC 17065** for certification bodies and **ISO/IEC 17025** for testing laboratories.

Official Designation

They are officially designated by a Member State and listed in the **NANDO** (New Approach Notified and Designated Organisations) database—the single source of truth for all Notified Bodies in the EU.

The Role of a Notified Body: Objective and Harmonized Evaluation


Manufacturer's Technical File & Product
Review
Test & Audit
Assess
Market Surveillance
EU Certificate of Conformity

Key Responsibilities

- **Perform Independent Evaluation:** Assess the product's cybersecurity against the CRA's essential requirements.
- **Review Documentation:** Scrutinize the technical file, test results, and risk analysis provided by the manufacturer.
- **Conduct Testing & Audits:** Perform hands-on testing, inspection, and auditing of systems and processes where required.
- **Issue Certificates:** If the product meets all requirements, issue an official EU certificate of conformity.
- **Support Market Surveillance:** May participate in ongoing activities to ensure certified products remain compliant in the market.

The Notified Body Certification Process in 5 Steps

Submission

The manufacturer submits a complete technical file and supporting documentation to the Notified Body.

Evaluation & Testing

The Notified Body performs its independent independent review, testing, and audits.

Certification

If successful, the Notified Body issues the certificate of conformity.

CE Marking

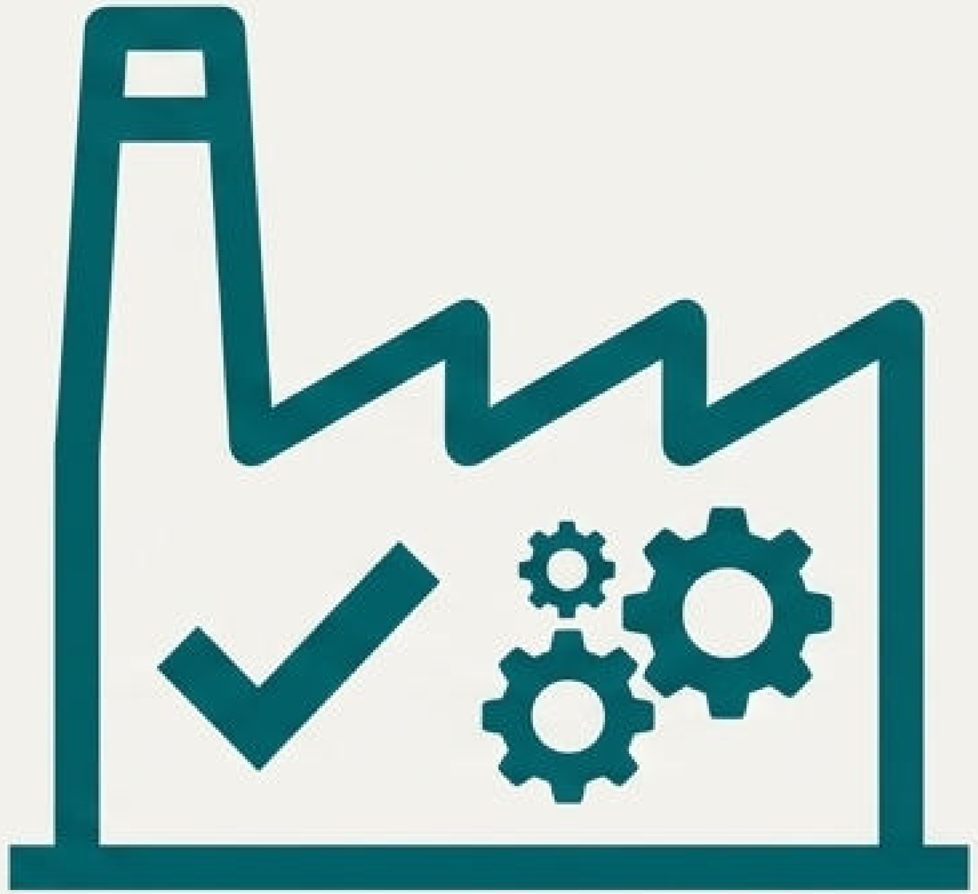
The manufacturer can now legally affix the CE marking to the product, signifying compliance.

Surveillance

The manufacturer must maintain compliance, subject to ongoing surveillance by the Notified Body and market authorities.

Path 2: Manufacturer Self-Assessment

In this pathway, the manufacturer performs its own conformity assessment without involving an external body. The manufacturer prepares the technical documentation, conducts the risk analysis, and declares under its **sole legal responsibility** that the product complies with the CRA.



- Based on internal controls and processes.
- Requires discipline and robust internal capabilities.
- Faster and more flexible than third-party certification.
- The manufacturer issues the final EU Declaration of Conformity.

Self-Assessment is Permitted Under Specific Conditions

This pathway is not available for all products. It is strictly reserved for circumstances where the cybersecurity risk is deemed manageable by the manufacturer.

- ✓ The product presents low or moderate cybersecurity risk.
- ✓ It does not handle critical functions or sensitive data.
- ✓ The manufacturer follows harmonized European standards published in the Official Journal of the EU.

> If these conditions are not met, or if relevant harmonized standards do not exist, certification by a Notified Body becomes mandatory.

Choosing Your Path: A Side-by-Side Comparison

Feature	Third-Party Certification (Notified Body)	Self-Assessment (Manufacturer)
Responsibility	Shared between manufacturer and Notified Body.	Solely on the manufacturer.
Verification	Independent, external verification provides high assurance.	No external verification of results.
Speed & Cost	Slower and more costly due to third-party engagement.	Faster time-to-market and lower direct costs.
Market Trust	High level of confidence from customers and authorities.	Trust depends heavily on the quality of documentation.
Ideal For	High-risk products, critical systems, products handling sensitive data.	Low-risk products, SMEs, rapid innovation cycles.

The Business Case for Self-Assessment

Faster Time-to-Market

Reduces delays associated with scheduling and engaging third parties.

Lower Costs

Eliminates fees for certification and auditing, a significant benefit for small and medium enterprises (SMEs).

Increased Flexibility

Allows for more agile development cycles, making it easier to manage updates and new product versions.

Understanding the Limitations and Responsibilities

Total Accountability

The manufacturer bears full legal responsibility for the product's compliance. Any failure rests solely with them.

No External Validation

The lack of a third-party review can lead to internal oversights or undiscovered vulnerabilities.

Potential for Scrutiny

Customers and market surveillance authorities may question the reliability of the assessment if documentation is weak, incomplete, or unconvincing.

Not Competitors, But a Complementary and Scalable System

The two conformity assessment pathways are designed to work together, creating a regulatory framework that is both robust and efficient.

Notified Bodies provide high assurance for complex or critical products where the impact of failure is severe.

Self-Assessment allows for efficiency and agility for the vast number of simpler, lower-risk products.

This makes the Cyber Resilience Act **flexible and scalable**, adapting cybersecurity assurance to each product's specific risk profile.

How Both Pathways Achieve the CRA’s Core Goals

Increase Transparency

Both pathways require detailed technical documentation, making cybersecurity practices more visible to authorities.

Build Confidence

A formal compliance mark (CE) backed by a clear process gives consumers and businesses confidence in the security of digital products.

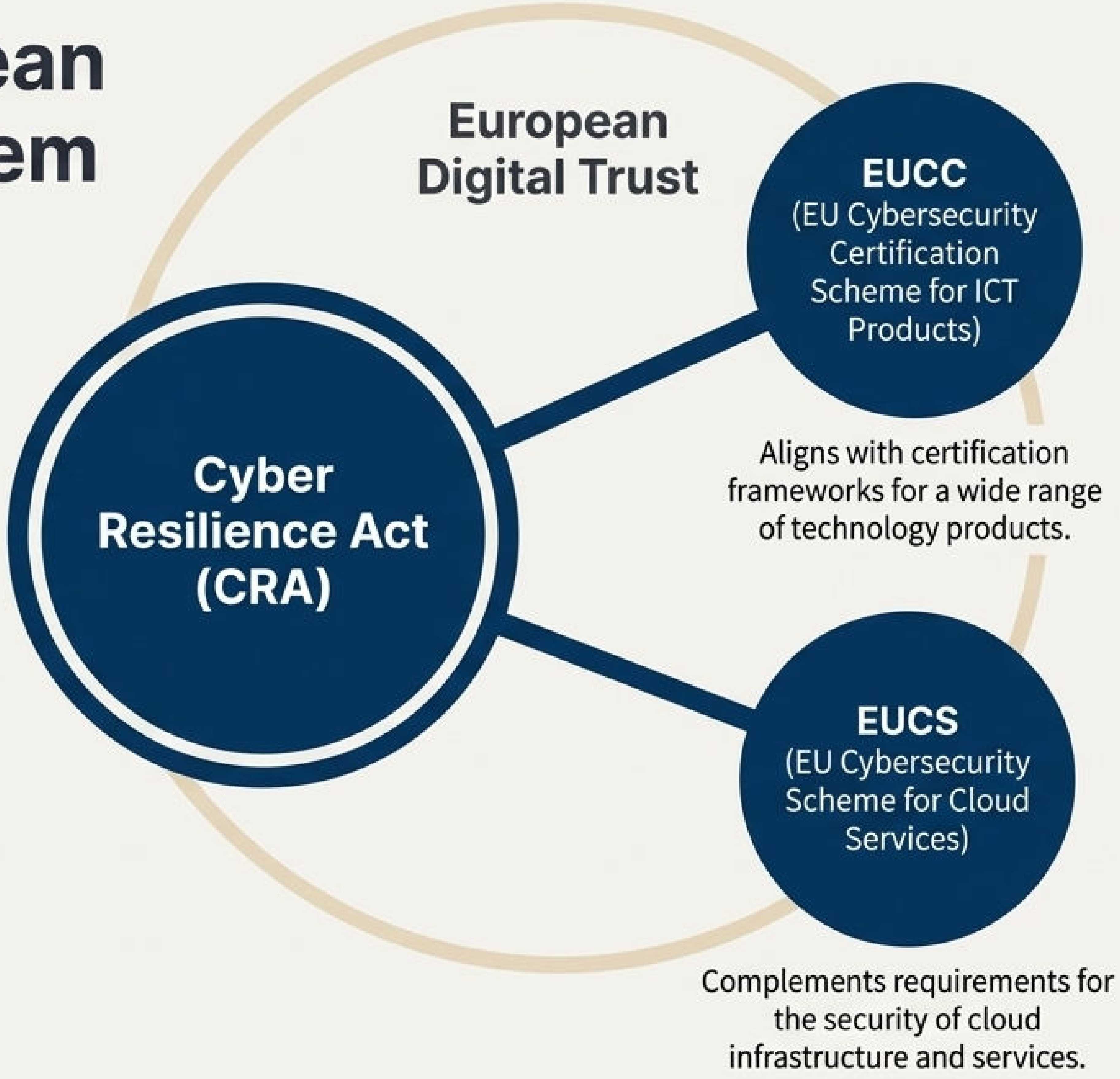
Enable Mutual Recognition

A certificate or declaration of conformity issued in one EU country is valid across the entire single market, removing trade barriers.

Part of a Unified European Cybersecurity Ecosystem

The conformity assessment framework of the CRA does not exist in a vacuum. It is designed to connect and align with other critical European cybersecurity schemes, creating a consistent and comprehensive approach to digital trust.

Together, these initiatives form a unified ecosystem, ensuring that cybersecurity requirements are applied fairly and consistently across the European Union, from individual products to complex cloud environments.


European Digital Trust
Cyber Resilience Act (CRA)
EUCC
(EU Cybersecurity Certification Scheme for ICT Products)
EUCS
(EU Cybersecurity Scheme for Cloud Services)

Aligns with certification frameworks for a wide range of technology products.

Complements requirements for the security of cloud infrastructure and services.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitev@dihtrakia.org

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools