Technology Strategy Board
Driving Innovation

Mitigating Supply Chain Risk Internationally

Paul Lewis

Lead Technologist – Network Security

National Defence | Défense nationale

Canada

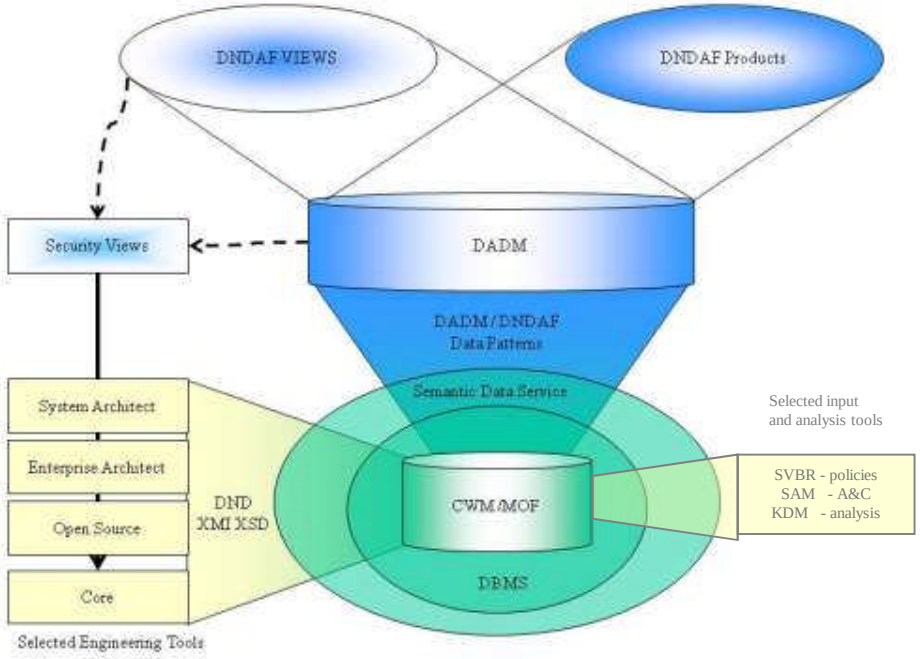
System Assurance in Support of the C&A Process

Presented by: Leslie Guyatt,
Project Director,
Enterprise Information Security Environment Project, Department of National Defence Canada

Information Management Group

Groupe de gestion de l'information

Leveraging OMG Standards: SwA Ecosystem+



Common Warehouse Metamodel (CWM)

Knowledge Discovery Metamodel (KDM)

Semantics of Business Vocabulary and Rules (SBVR)

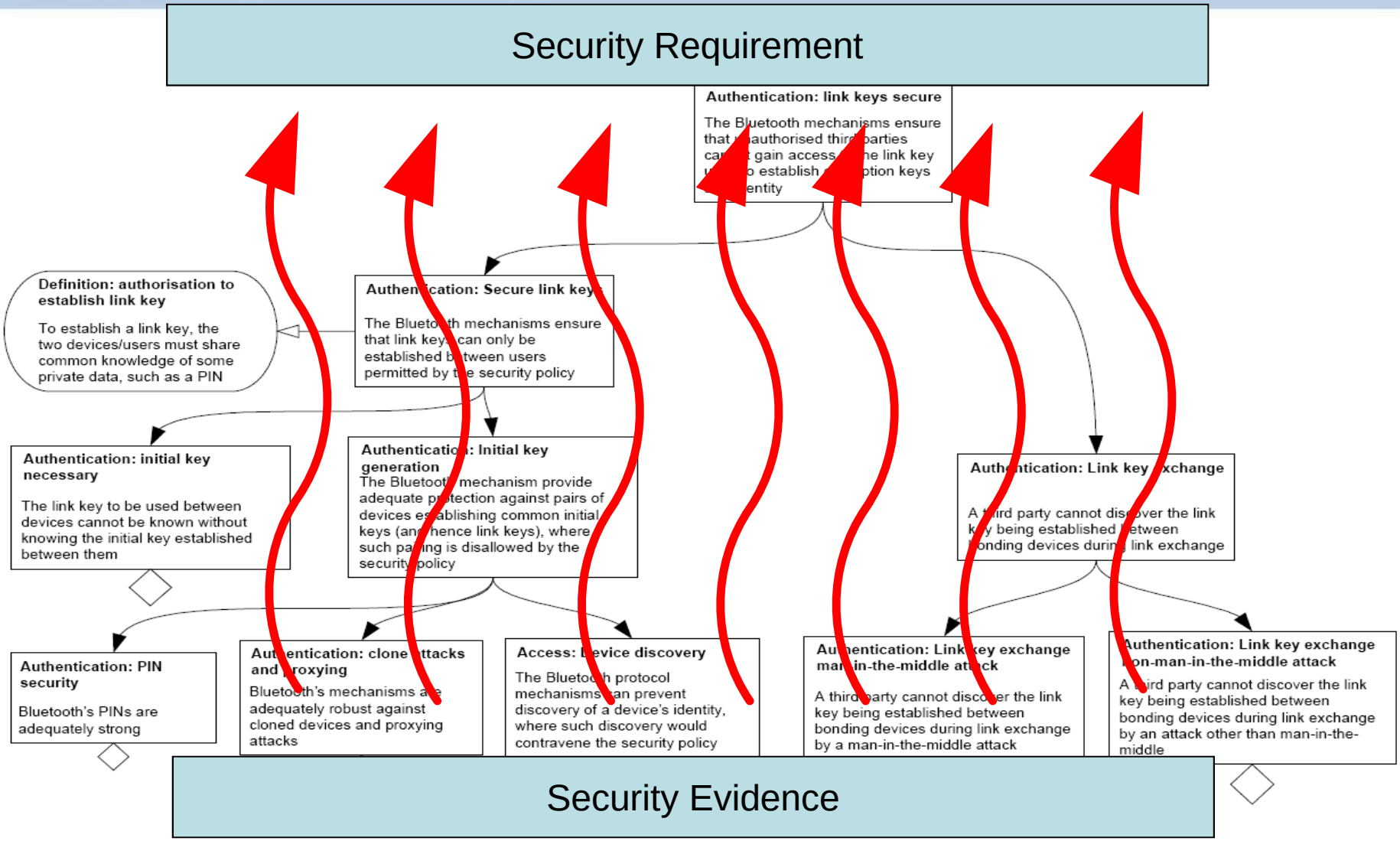
Software Assurance Metamodel (2 standards – WIP)

Unified Profile for DoDAF/MODAF (UPDM**)**

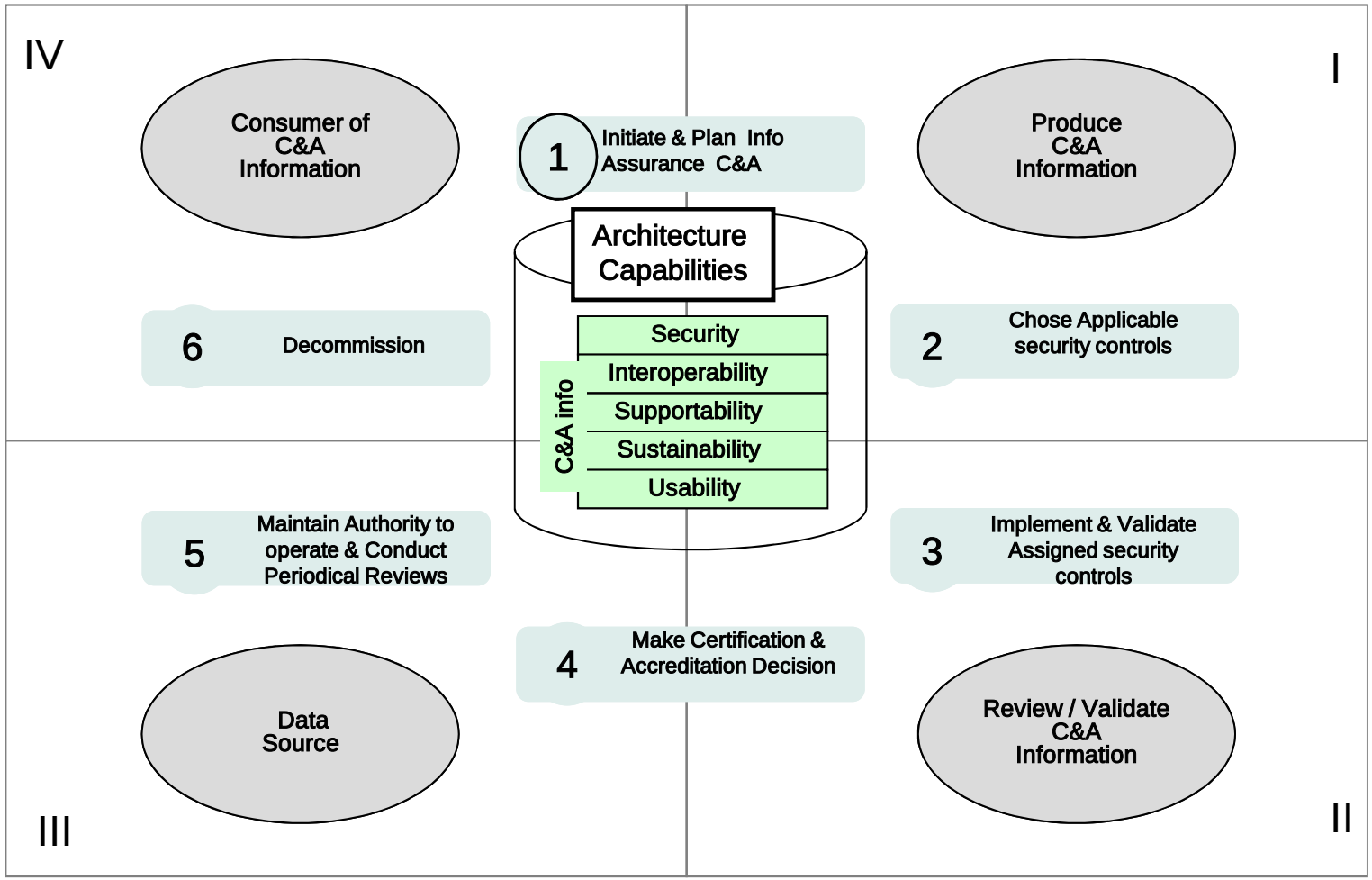
Information Security Objectives

- Establish standard based, Assurance Framework to enable automated, consistent, repeatable C&A process
- The Assurance Framework provides common and consistent guidance and communications
  - Capturing a goal-aligned traceability Model
  - Obtaining fact based evidence
  - Assessing residual risk based on discovery non-compliance parts

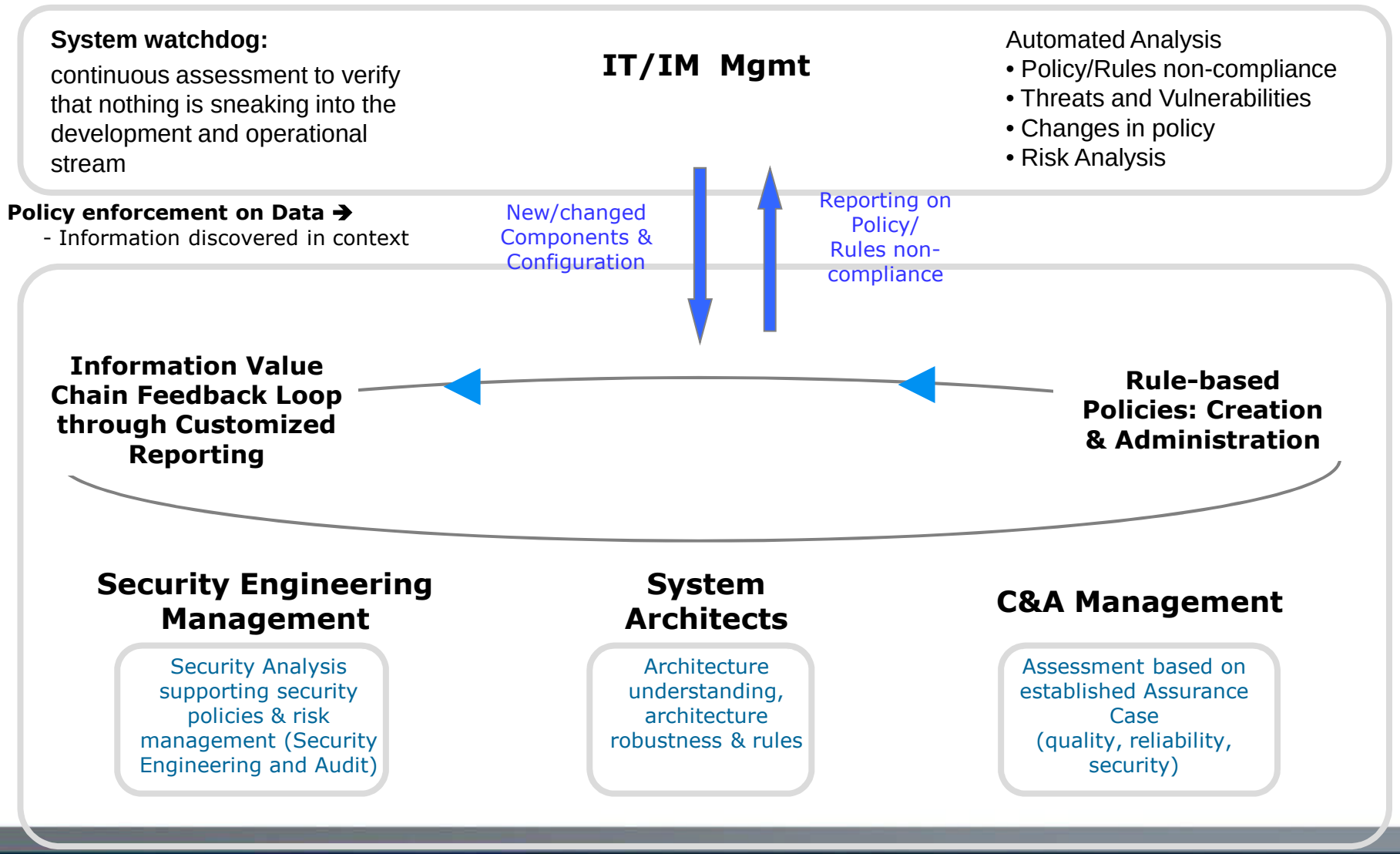
A Simple Assurance Case Structure



C&A Process with the Traceability Model



Achievable Continuous Assurance



Technology Strategy Board
Driving Innovation

Secure Software Development Partnership (SSDP)

Setup to deal with the challenge of secure software development and design

Founded by :

•Technology Strategy Board (TSB) and
•The Centre for Protection of National Infrastructure (CPNI)

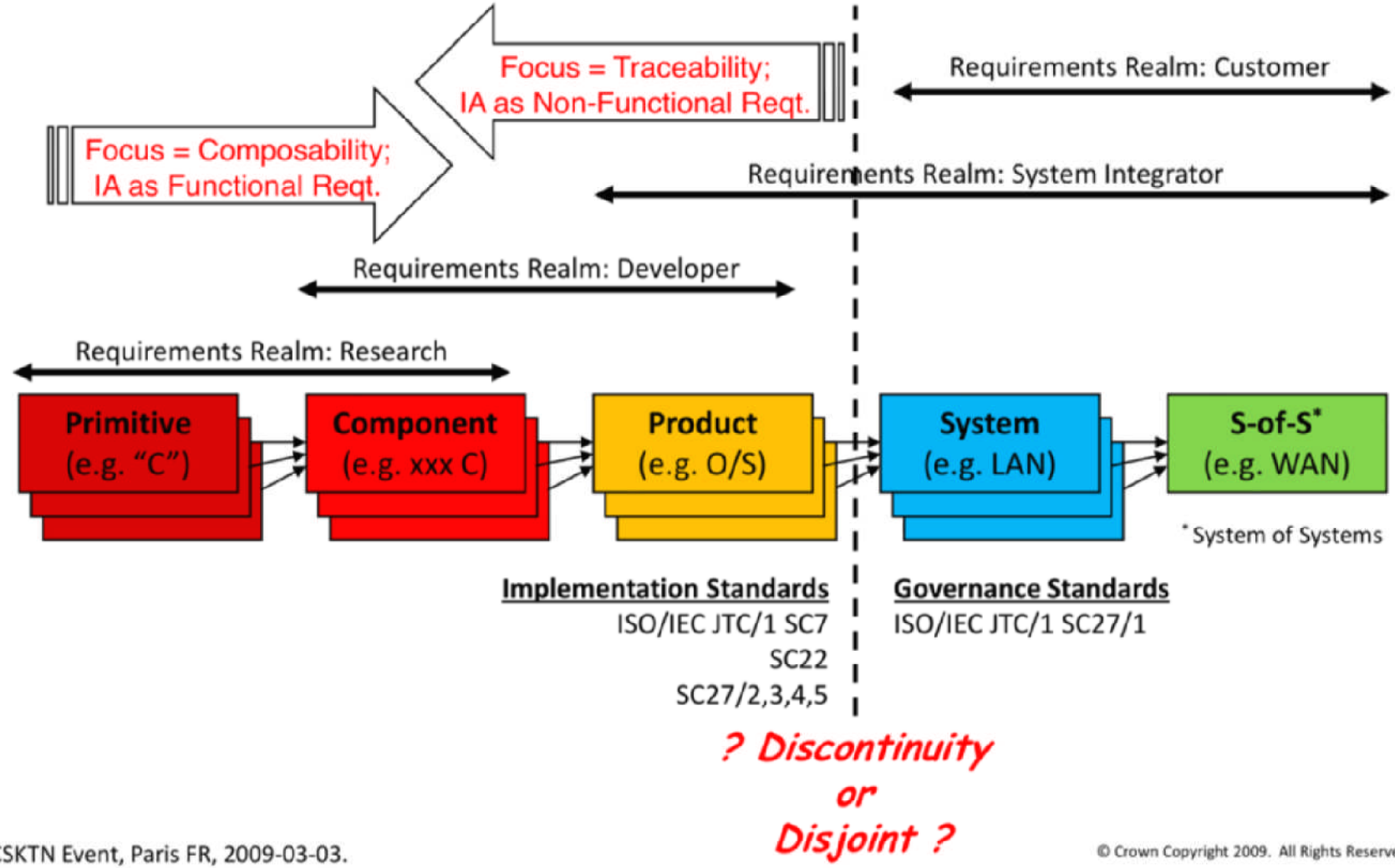
CPNI
Centre for the Protection of National Infrastructure

A partnership consisting of a tripartite of business, government and academic organisations.

Currently 60 organisations involved.

- **Environmental shaping**, including business models, markets, supply chains and consumer demand.
- **Concept and process development**, including information exchange, risk based processes, requirements capture, whole life processes and validation.
- **Technical facilitation**, including modelling, analytical tools and technical standards.
- **Professionalisation**, including independent architects, standards, curriculum design, competencies and good practices.
- **Communications**, including the development and measurement of awareness and education campaigns.

Challenges to building in ... information security, privacy and assurance



Priority Areas:

The creation, maintenance and publication of a catalogue of case-study material that provides supporting evidence and precedent for business case preparation.

Create an environment to increase the percentage of computing undergraduates obtaining basic awareness of software security issues, rather than increasing the duration of existing programmes.

Office of Government Commerce to create software procurement guidelines that include secure software development requirements.

Development of Standards, in particular in providing input to International Standards Organisations.