

# KDM Analytics™



Software Assurance Ecosystem Infrastructure

## **Djenana Campara**

Chief Executive Officer, KDM Analytics

Board Director, Object Management Group (OMG)

Co-Chair Software Assurance and Architecture Driven  
Modernization, OMG

# Agenda

- √ Software Assurance (SwA) and Enabling Technologies
- √ Introduction to OMG SwA Special Interest Group and Its Current Work
  - √ Introduction to SwA Ecosystem
  - √ Ecosystem Values
  - √ Overview of OMG Specifications that are Key Contributors to SwA Ecosystem
- √ Upcoming OMG SwA Events
- √ Contacts

# Software Assurance

- v Definition of SwA
  - v The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software (NDIA whitepaper)
  - v The justifiable trustworthiness in meeting established business and security objectives (OMG whitepaper)
- v Why Software Assurance is Critical
  - v Software and the processes for acquiring and developing software represent a material weakness
  - v No Software is an island – can not be developed in isolation
    - v As software organizations recognize the need to evolve their systems beyond homogeneous and monolithic solutions to ones with a netted approach to architectures supporting COTS, multi-operating environments and multiple languages - security has become a significant challenge
    - v One rotten apple spoils the whole barrel
- v Simultaneously, the tooling industry which provides enabling technologies to build secure software systems has not kept pace with the software system evolution
  - v a large gap has been created in which point tools have not kept pace nor provide the comprehensive evaluation required for a significant portion of the software industry, causing even greater security exposure

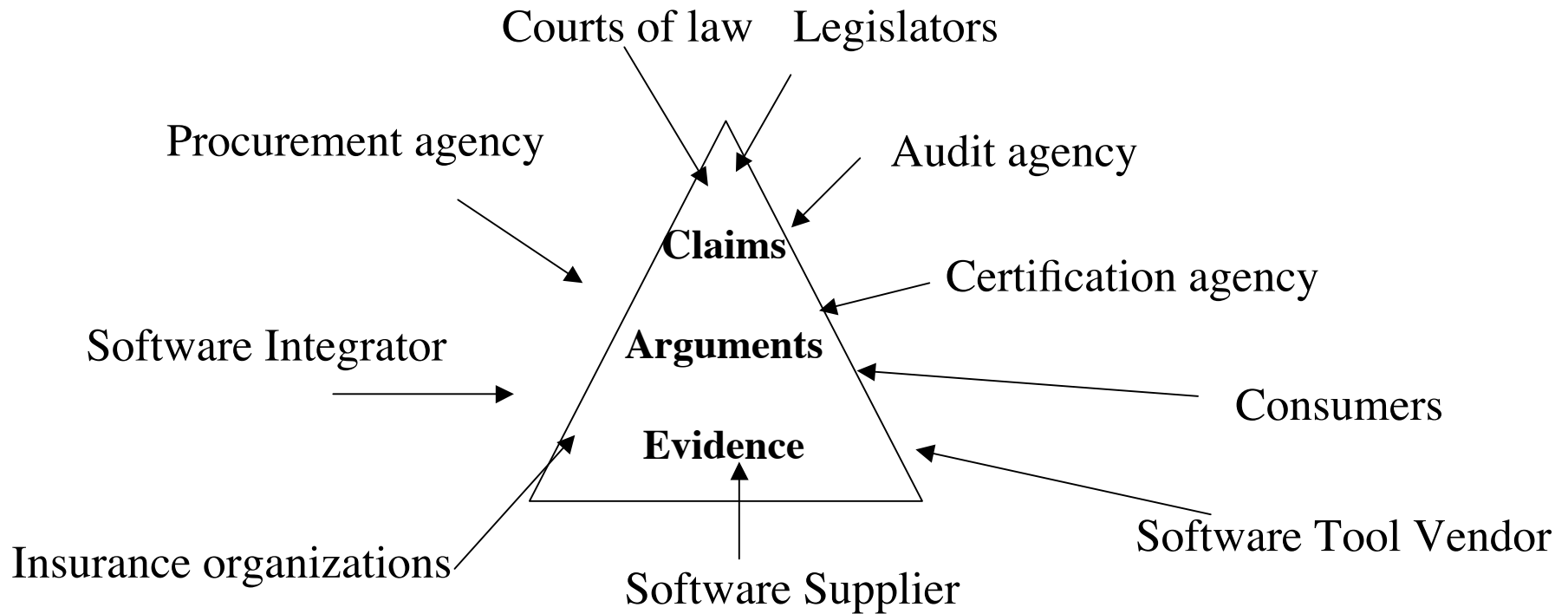
# *Current State of the Software Assurance Industry*

- v Widening the gap further, software communities, in an effort to increase system security, focused their efforts on the development/compliance to more standards and guidelines on software systems, ignoring the evolution of technologies that can enable organizations to cost effectively implement and certify against said standards causing
  - v More standards but less standardization
  - v Less standardization leading to less confidence that products are trustworthy
  - v Less confidence leading to lower levels of assurance
- v SwA Landscape shows big gap in area of enabling technologies
- v Realizing Software Assurance is about enabling industry and government to **leverage** and **connect** existing standards, policies, practices, processes and tools, in an affordable and efficient manner resulting in
  - v Increased level of confidence through justified trustworthiness

# *Increasing Confidence through Justified Trustworthiness*

- ✓ Justifiable trustworthiness delivered through software assessment
  - ✓ Result of software assessment is presented as Assurance Case: “A reasoned, auditable argument created to support the contention that a defined system will satisfy the particular requirements,” with supporting evidence.
- ✓ An assurance case is created to justify claims of meeting required security properties through a structure of sub-claims, arguments, and supporting evidence
- ✓ Two potential purposes of assurance case are to show that the specified security properties are
  - valid (result in meeting real world intentions and expectations)
  - the system as designed and built meets its specified security properties.
- ✓ These two points must be addressed – implicitly or explicitly – by any sound approach to engineering (or using) software or to managing risk where security is an issue
- ✓ Documenting the relevant arguments and supporting evidence so they can be reviewed and analyzed is useful and prudent

# Participants in Software Assurance



**All participants exchange assurance case information**

# Software Assurance Special Interest Group (SwA AB SIG)

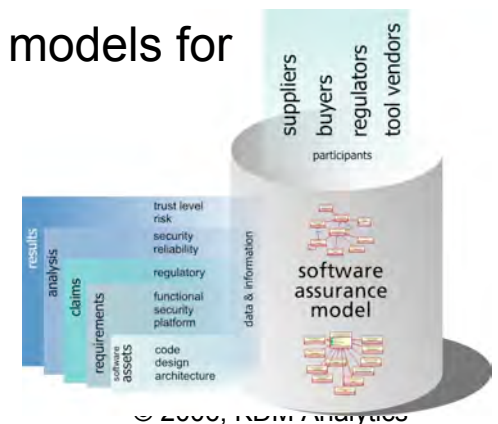
## ✓ Mission

- ✓ to establish a common framework for analysis and exchange of information related to software trustworthiness.

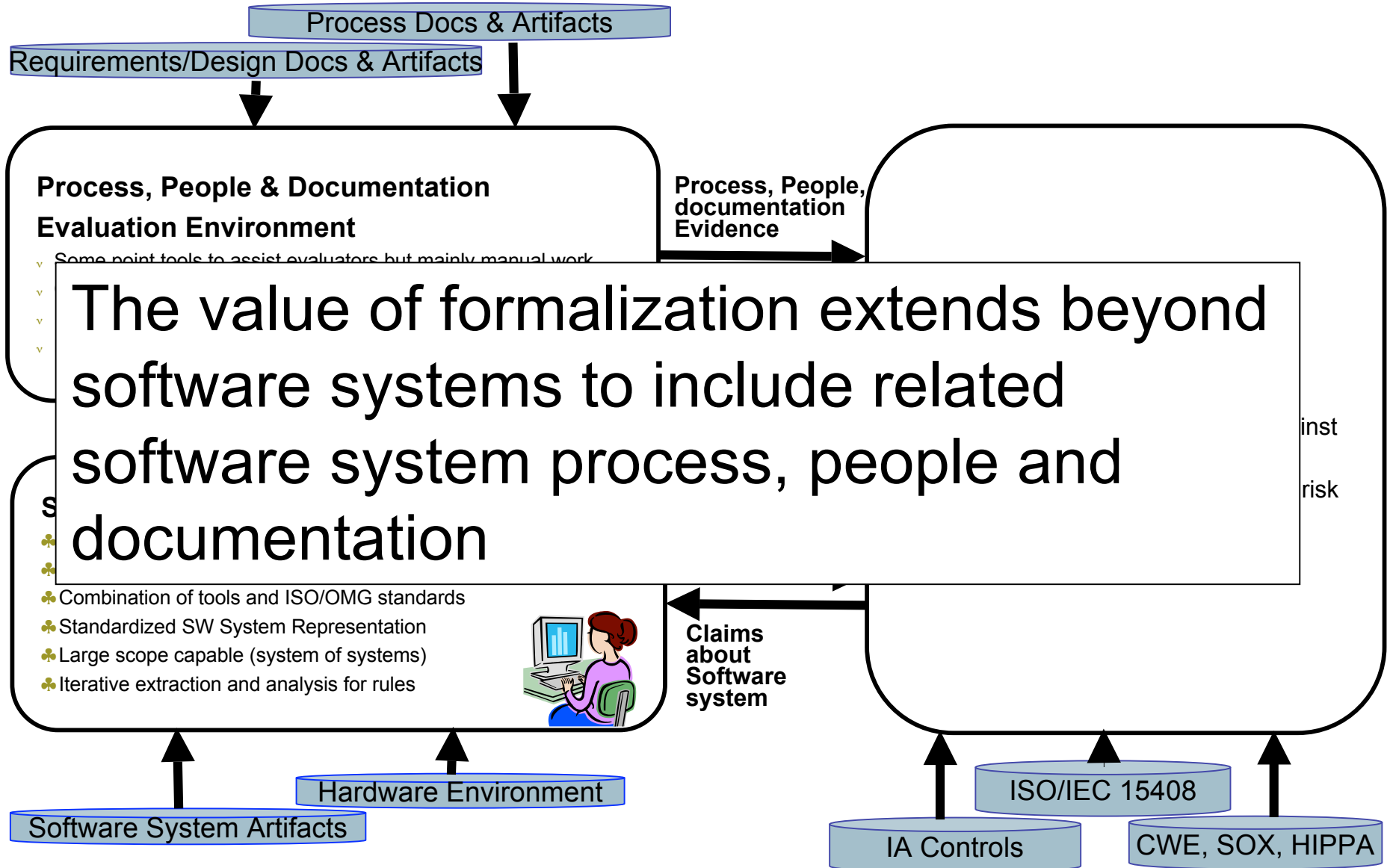
## ✓ Goals

- ✓ Facilitate the development of a specification for a Software Assurance Framework
  - ✓ Enable industry and government to **leverage** and **connect** existing standards, policies, practices, processes and tools, in an affordable and efficient manner
  - ✓ Enable industry to develop automated tools that support the common framework to make SwA activities highly automated and cost-effective
- ✓ Leverage other related OMG specifications such as KDM, SBVR, ...
- ✓ Find ways to leverage the various quality and maturity models for security with OMG specifications.

**Standardization will ensure that all participants are investing not just in individual activities but in a coordinated strategy.**



**Software Assurance Ecosystem:** A formal framework for analysis and exchange of information related to software security and trustworthiness



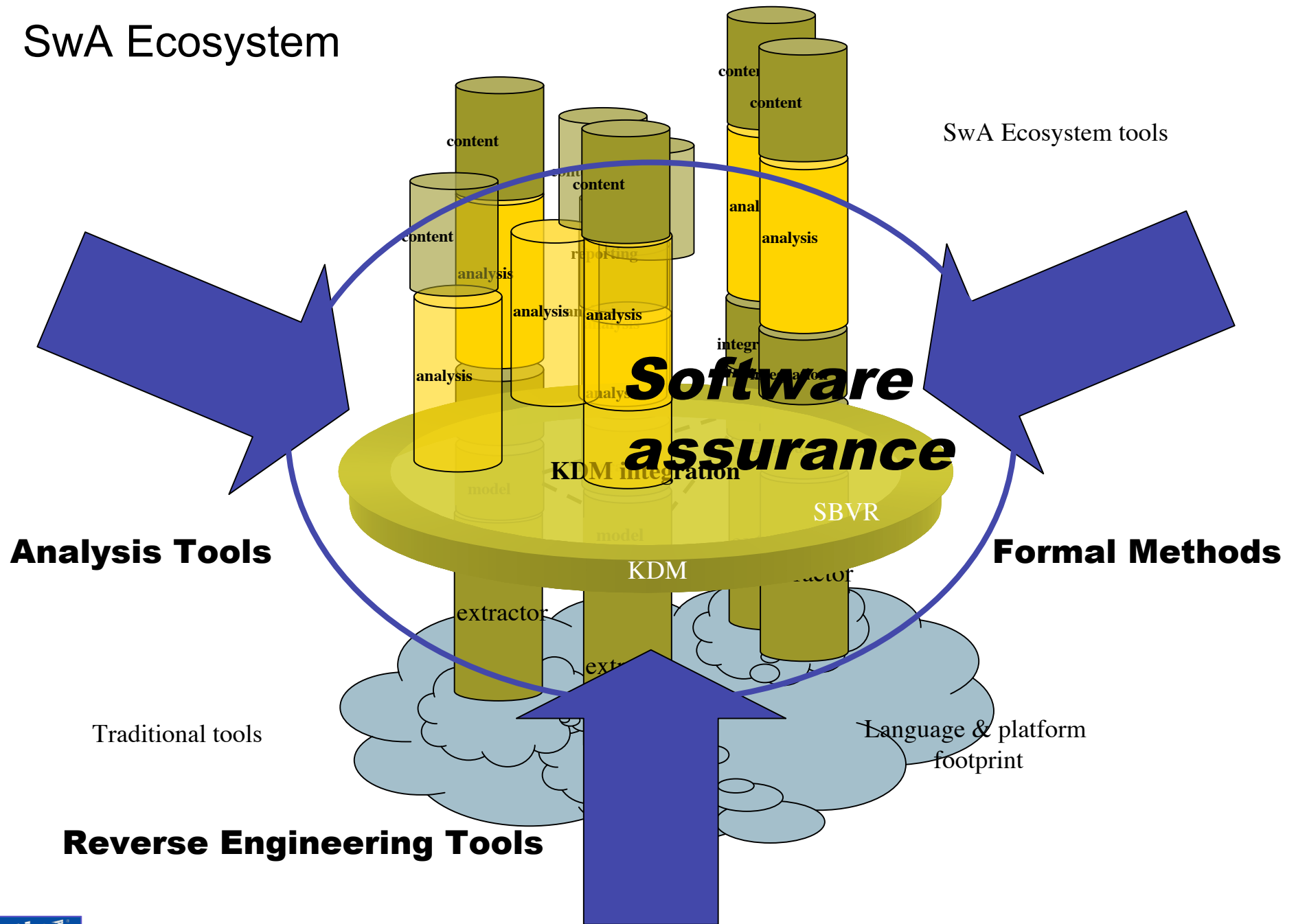
# *Ecosystem Values*

- √ Formal Representation of Claims, Arguments and Evidence
  - √ Provides precise and unambiguous specification
    - √ Legal and contractual agreements
    - √ Can generate documents and reports
    - √ Excellent communications vehicle between client and evaluator
  - √ Builds a repository of Claims and Arguments (reusable)
  - √ Improves objectiveness, accuracy of evidence collection through process, people, documents
- √ Highly automated collection of Evidence in relation to direct claims against software systems
- √ Software Assurance Repository brings all Evidence together with the Claims
  - √ Improves evaluations
    - √ Evaluations are consistent, objective and with repeatable results across different labs
    - √ Can easily and quickly look across all evidence to build a correlation model as continuous improvement of assessments
    - √ Automated validation of claims against evidence based on arguments
  - √ Highly automated and improved risk assessments using transitive inter-evidence point relationships

## OMG SwA SIG Focus

- v Software Assurance Ecosystem focuses on
  - v Framework for exchange of information related to claims, arguments and evidence
    - v Revised whitepaper due to December 2006
    - v Currently we are in the process of collecting requirements for Evidence Metamodel
      - v The first draft of mandatory requirements presented in the last meeting, Sep. 28
  - v Framework for automated collection of evidence
    - v The key enabler is the Software Assurance (SwA) Ecosystem infrastructure, which is an open standard-based integrated tooling environment that dramatically reduces the cost of software assurance activities
      - v It integrates 3 different communities: Formal Methods, Reverse Engineering and Static Analysis to complete SwA enabling technology solution
      - v Enables different tool types to interoperate
      - v Besides expanding market for known players, it introduces many new vendors to ecosystem because they each have parts of the tool chain (and may not realize it). Eg. IBM, Telelogic, Borland ASG, Relativity and others)

# SwA Ecosystem



# *Software Assurance Ecosystem Main Specifications*

- v Semantics of Business Vocabulary and Rules (SBVR)
  - v Language for expressing Claims, Arguments and Evidence
  - v Excellent representation of requirements/policies in an easy to understand but formal manner
  - v Precise and un-ambiguous
  - v Used for both software system requirements and for software process, people and documentation requirements (eg. Completely covers IA Controls and Protection Profiles)
  - v Defining SwA vocabulary within SBVR framework – work part of the rollout plan

## *Software Assurance Ecosystem - Main Specifications (Cont.)*

- √ Knowledge Discovery Meta-model (KDM)
  - √ A framework for documenting and formally representing existing software assets and their operational environment
    - √ Abstracted from source code for language independence
    - √ Directly supports structure and architecture models
    - √ Directly supports business rule and security policy abstractions
  - √ Acts as a checklist/requirements for what needs to be documented
  - √ Input can be provided manually (services) or automatically (tools)
  - √ Supports export and import of data currently contained within individual tool models that represent existing software assets. This facilitates continuous interoperability between existing SwA tools

# *Software Assurance Ecosystem - Main Specifications (Cont.)*

- v Software Assurance Meta-model (SAM)
  - v Work in progress at OMG
  - v A repository structure for representing and exchanging Claims, Arguments and Evidence
  - v Claims, Arguments and Evidence are documented using SBVR
  - v A framework for building SwA related tooling for:
    - v Improving repeatability and objectiveness of evaluations by automatically connecting evidence and claims
    - v Greatly improving risk assessments through evidence correlation
    - v Managing claims for consistency, understanding gaps, duplication, etc.

## *Upcoming OMG Events*

- √ Mar. 5-7, 2007; Washington DC
  - √ Software Assurance Workshop
  - √ <http://www.omg.org/news/meetings/SWA2007/call.htm>
  
- √ Mar. 26-30, 2007; San Diego, CA
  - √ OMG Technical Meeting – Software Assurance AB SIG

# Contacts

- √ All presentations will be posted at our website
  - √ <http://swa.omg.org>
  
- √ Any questions can be directed to OMG SwA co-chairs
  - √ J.D. Baker, BAE - [james.d.baker@baesystems.com](mailto:james.d.baker@baesystems.com)
  - √ Djenana Campara, KDM Analytics – [djenana@kdmanalytics.com](mailto:djenana@kdmanalytics.com)