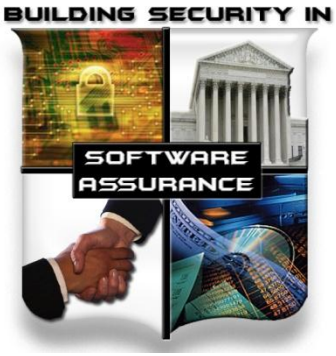
Homeland Security

Commerce

National Defense



Standards Activities

Making Security Measurable™

Robert A. Martin
28 Feb 2011

MITRE

Cybersecurity Standards:
A Marrage of Cognitive and Cyber Speed Activities & Info

- CVE identifiers require analysts to investigate/correlate…
  - Which enables tools to correlate at cyber speed…
- OVAL definitions require analysts to define criteria…
  - Which enables checking systems for user defined content at cyber speed…
- CVSS scores require analysts to assign vector values…
  - Which enables identifying severity and following a priori guidance on risk tolerance at cyber speed…
- CPE names require vendors/analysts to assign names…
  - Which allows correlating platform information at cyber speed…
- CCE identifiers require analysts/vendors to identify controls…
  - Which allows correlating settings with desired settings at cyber speed…
- XCCDF requires analysts to craft policy statements…
  - Which allows multiple tools to follow and report against user defined content at cyber speed…
- OCIL requires analysts to craft questionnaires…
  - Which allows multiple tools to ask and report against user defined content at cyber speed…
- CWE requires analysts to create content about weaknesses, impacts, mitigations…
  - Which enables tools to correlate at cyber speed…
- CWSS requires analysts to describe the context specific factors to prioritizing weaknesses
  - Which enables tools to directly give tailored rankings of findings for any specific application…
- CAPEC requires analysts to document the individual components of attacks…
  - Which enables correlation of observations at cyber speed and recreation of attacks as test cases…
- MAEC requires analysts to document the variety of characteristics of malware…
  - Which enables adhoc integration and interoperability of tools, repositories, and analysts as needed…

Example: SCAP's Automation Requires

- Consistent input from Cognitive activities feeding SCAP
- Structured input & output to and from those Cognitive activities
- Universal definition of concepts across SCAP elements

Cognitive Speed

Content/Guidance Writing

Enumeration Assignment

Cyber Speed

Assessment by SCAP enabled Tools

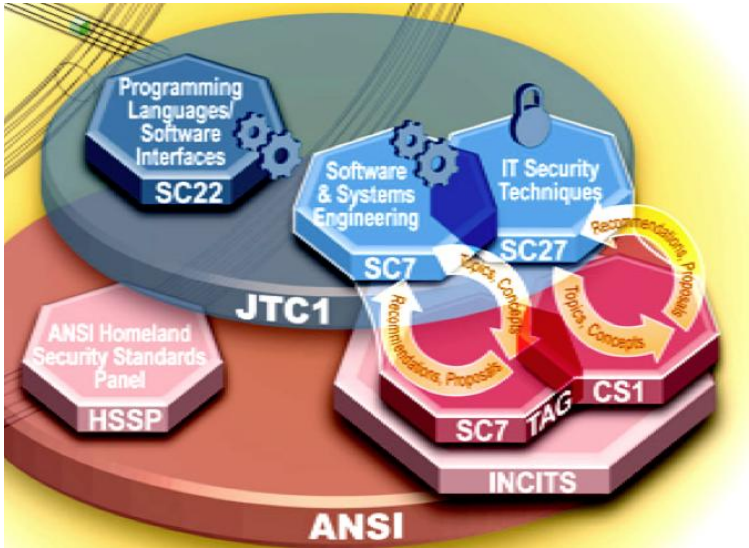
Cognitive Speed

Enterprise Security Management

What Standards Groups are Involved in Cybersecurity?

Illustration from OSD Supply Chain Risk Management Office courtesy of BAH

What Standards Groups Have Efforts Focused on Cybersecurity and Assurance?



Assessment Languages (XCCDF/OVAL/OCIL)

Assessment Languages

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

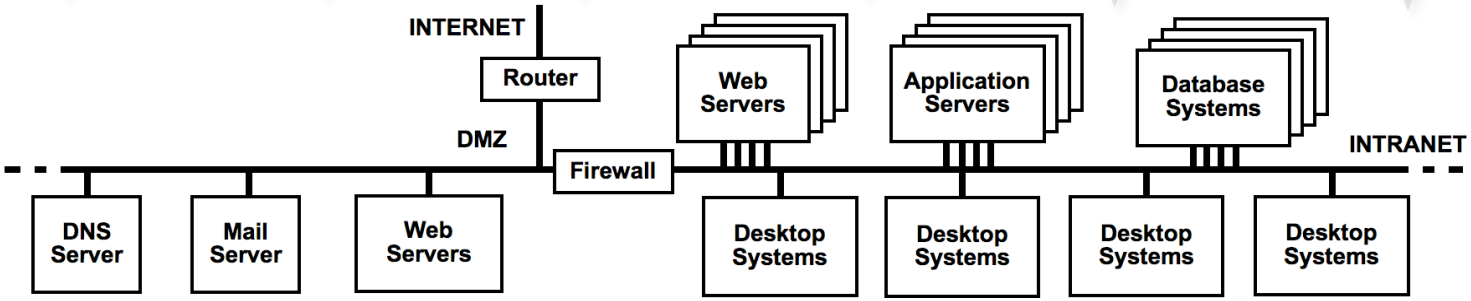
Threat Analysis

Intrusion Detection

Incident Management

Operations Security Management Processes

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation



Operational Enterprise Networks

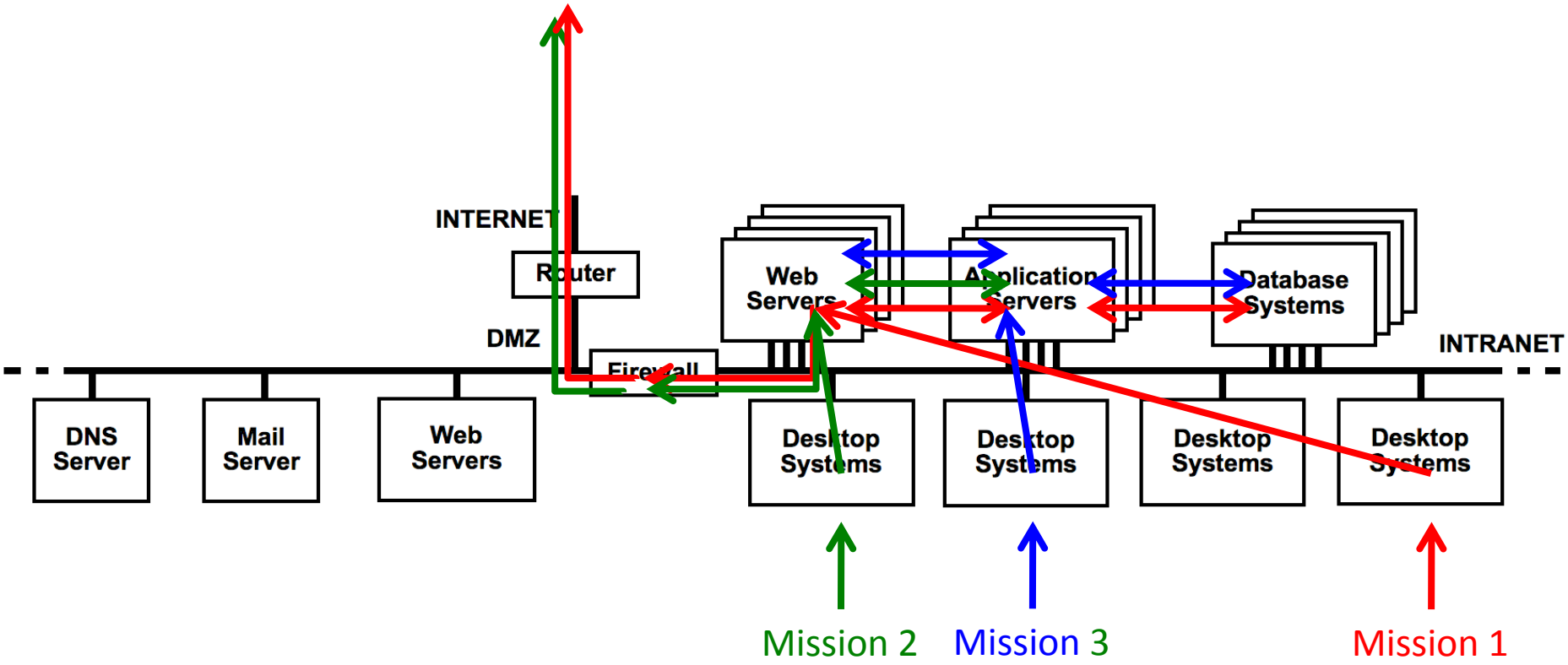
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

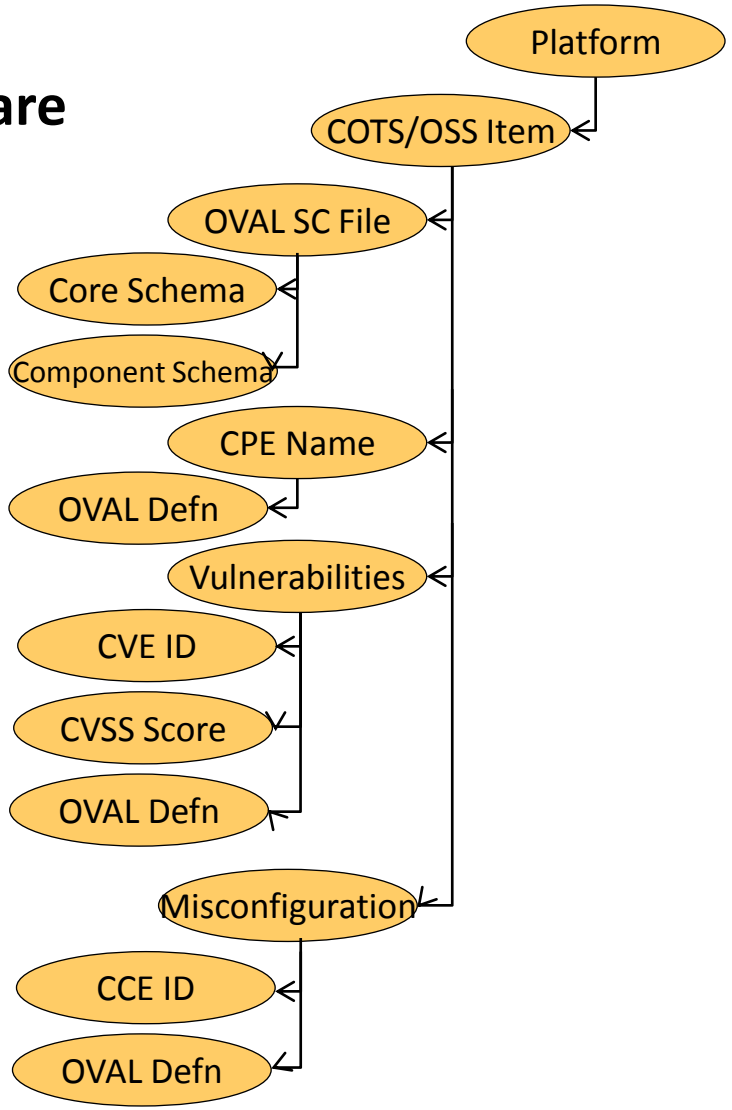
Enterprise IT Asset Management

Enterprise Information Technology Infrastructures Are There to Support Missions and Enterprise Capabilities



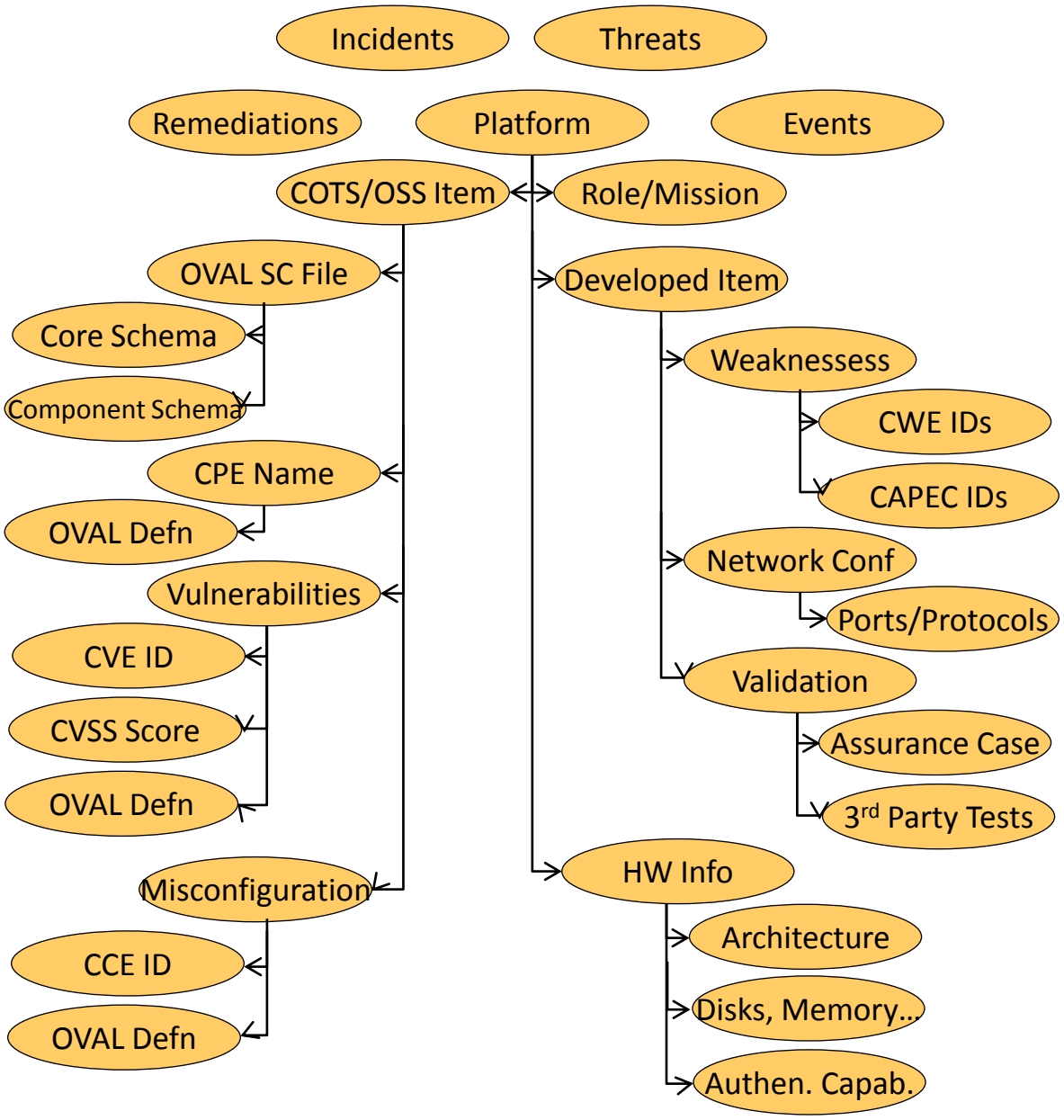
Assessment Languages and the model beneath them…

- A platform:
  - Commercial or Open Source Software
    - OVAL Systems Characteristics File
      - Core Schema
      - Component Schema
    - CPE names
    - Vulnerabilities
      - CVE identifiers
      - CVSS scores
      - OVAL definitions
    - Misconfigurations
      - CCE identifiers
      - OVAL definitions

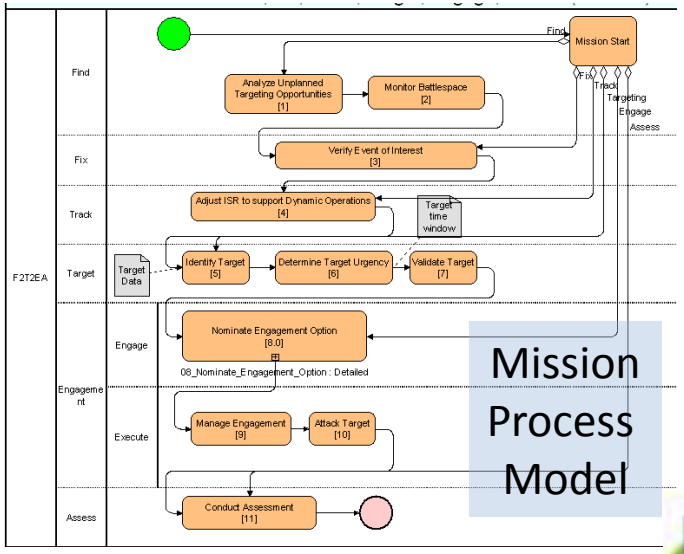


Other things to model…

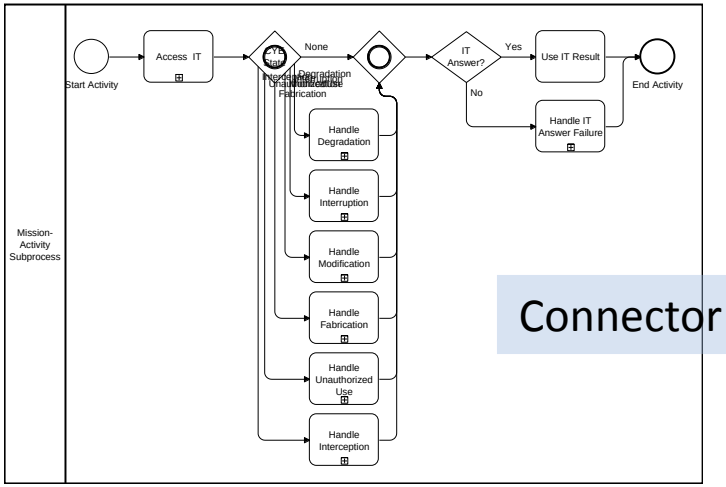
- A platform:
  - Role/Mission
  - Hardware Information
    - Architecture
    - Disks, Memory, Comms, Input Devices
    - Authentification Capabilities
  - Organically Developed Software
    - Weaknesses Evaluated For
      - CWE IDs
      - CAPEC IDs
    - Validation Methods
      - Structured Assurance Case
      - 3rd Party Testing
  - Network Configuration Information
    - Ports/Protocols Settings



Mission Modeling: using BPMN (Business Process Modeling Notation) to represent missions and their cyber dependencies

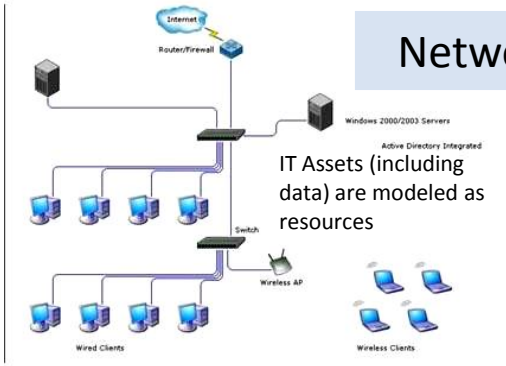


Mission Process Model



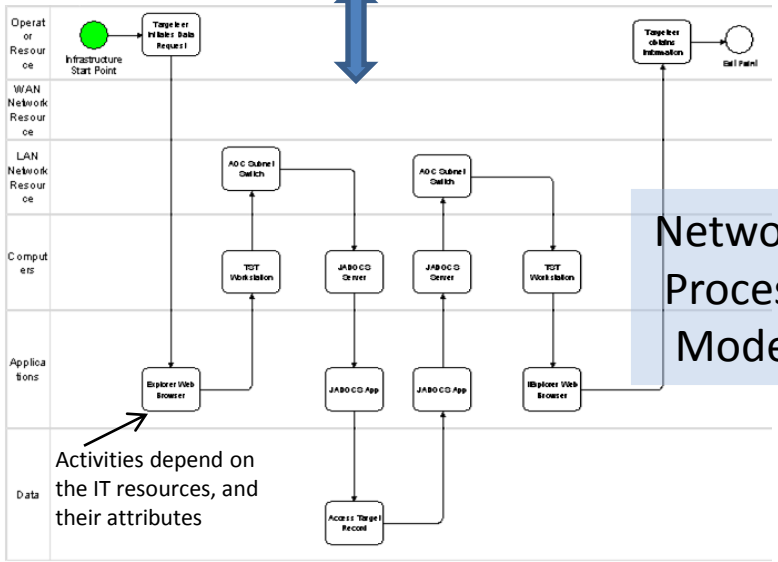
Connector

BPMN



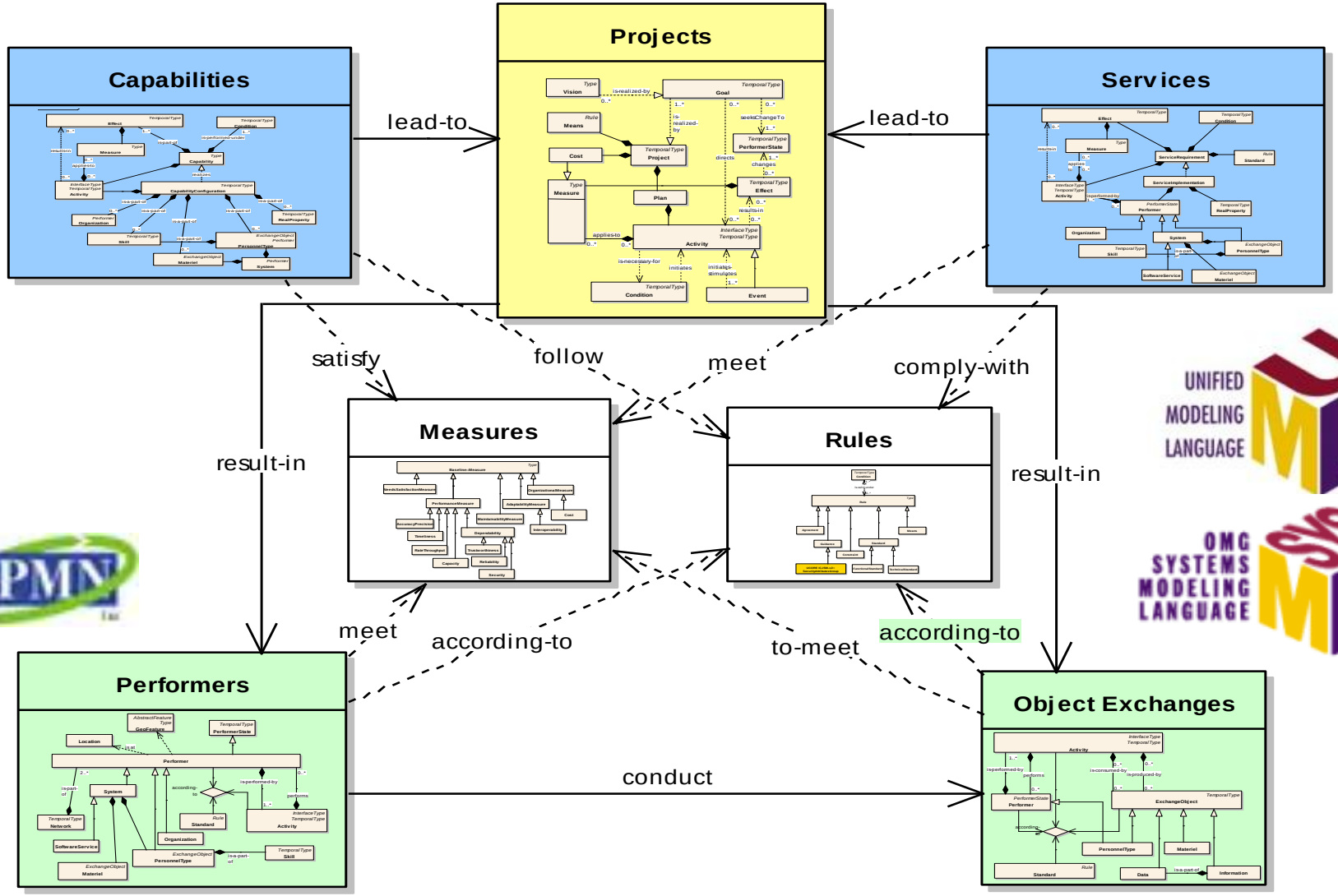
Network Diagram

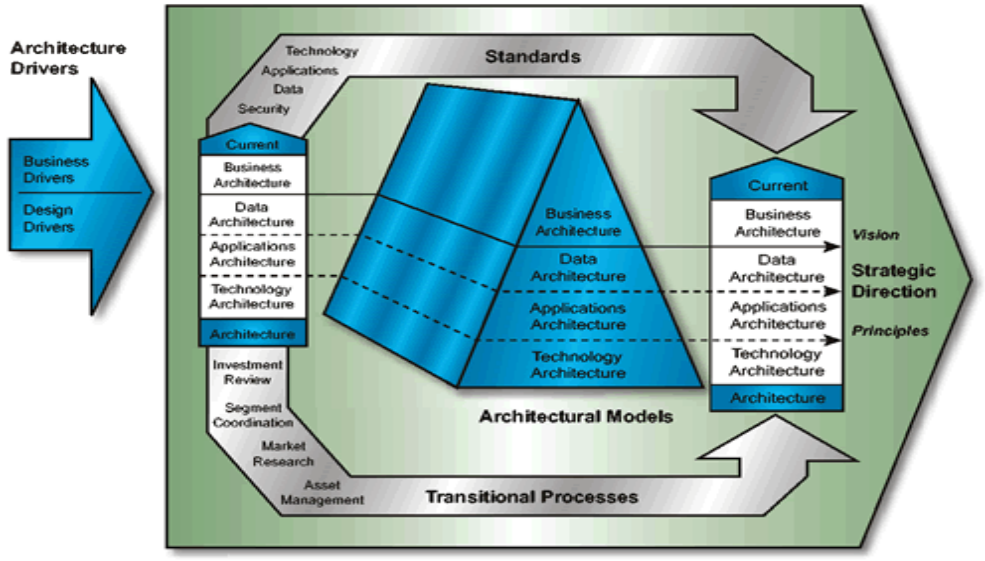
IT Assets (including data) are modeled as resources



Network Process Model

DoD Architecture Framework (DoDAF) V 2.0 Metamodel

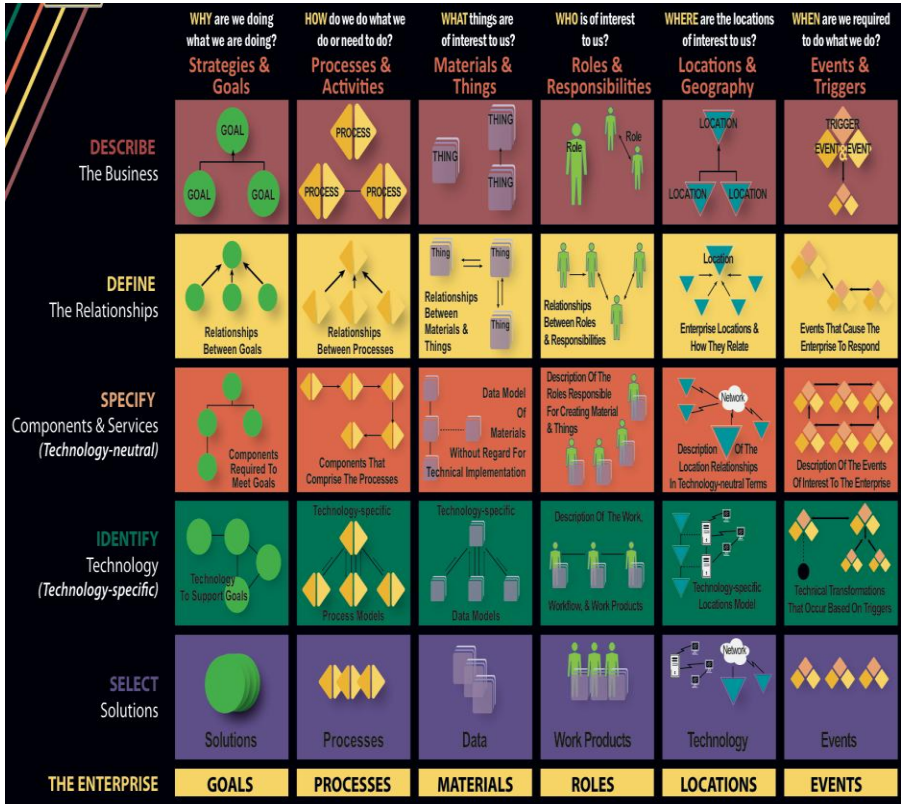




Federal Enterprise Architecture Framework (FEAF)

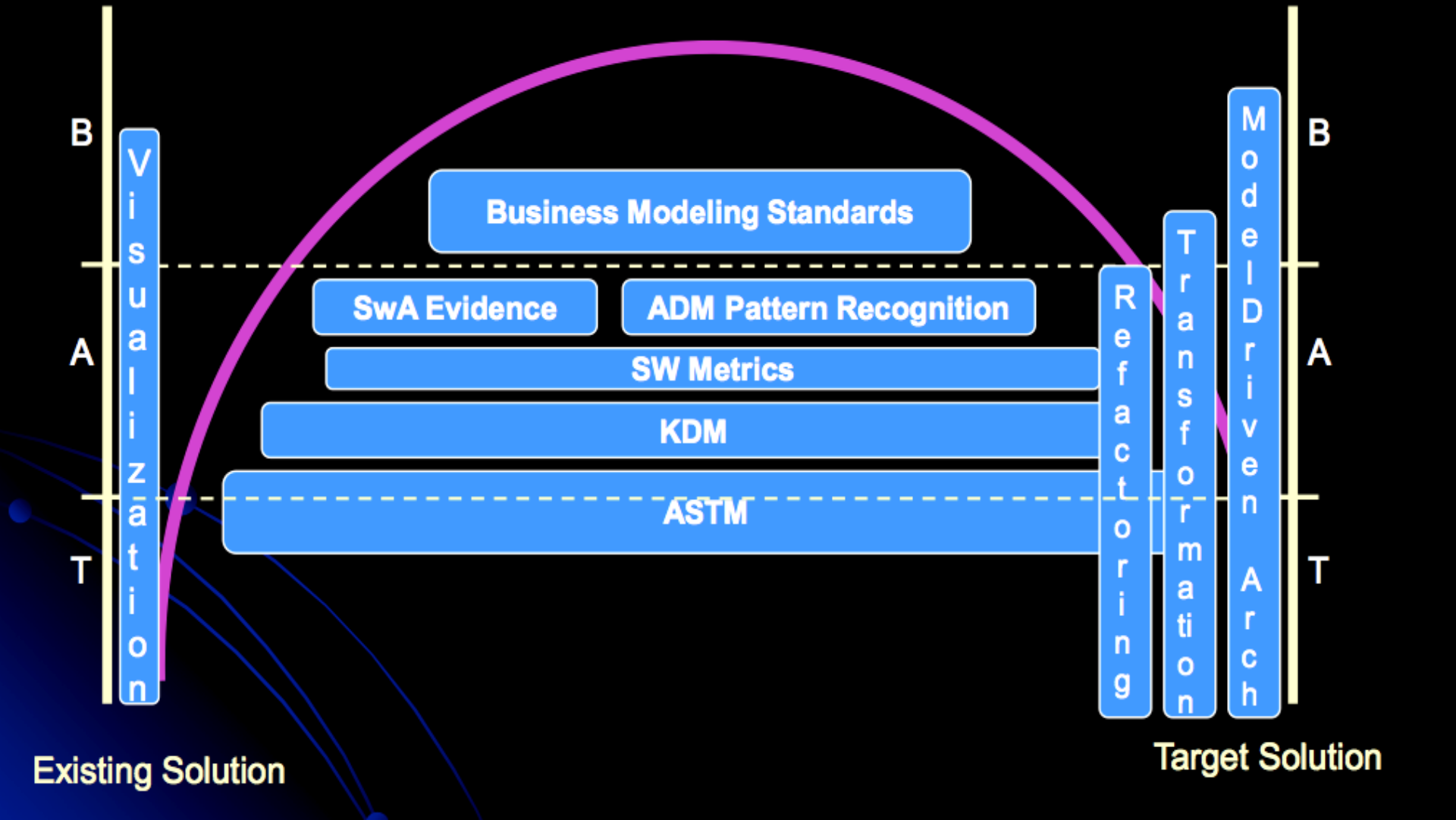
The Zachman Framework	DATA *What (Things)*	FUNCTION *How (Process)*	NETWORK *Where (Location)*	PEOPLE *Who (People)*	TIME *When (Time)*	MOTIVATION *Why (Motivation)*
SCOPE (Contextual) *Planner*	List of things important to the business	List of processes the business performs	List of Locations in which the business operates	List of Organizations important to the Business	List of Events significant to the Business	List of Business Goals/Strategies
BUSINESS MODEL (Conceptual) *Owner*	Semantic Model: Common Warehouse Metamodel	Business Process Model	Business Logistics System: Business Process Definition (Planned)	Work Flow Model: EDOC	Master Schedule	Business Plan: Business Rules (Planned)
SYSTEM MODEL (Logical) *Designer*	Logical Data Model	Application Architecture: EDOC	Distributed System Architecture: EAI Profile	Human Interface Architecture: UML Web Profile	Processing Structure: Scheduling Profile	Business Rule Model
TECHNOLOGY MODEL (Physical) *Builder*	Physical Data Model: (CWM)	System Design: NET EJB CORBA	Technology Architecture: NET EJB CORBA	Presentation Architecture	Control Structure	Rule Design
DETAILED REPRESENTATIONS (Out-of-Context) *Sub-Contractor*	Data Definition	Network Architecture	Network Architecture	Security Architecture	Timing Definition	Rule Specification

UML



Object Management Group – Architecture Driven Modernization TF & Systems Assurance TF

ADM Standards Span the Entire IT Architecture Spectrum



SC7 WG3

ISO/IEC JTC 1/SC 27 **NXXXX**

ISO/IEC JTC 1/SC 27/WG x **NXXXXX**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

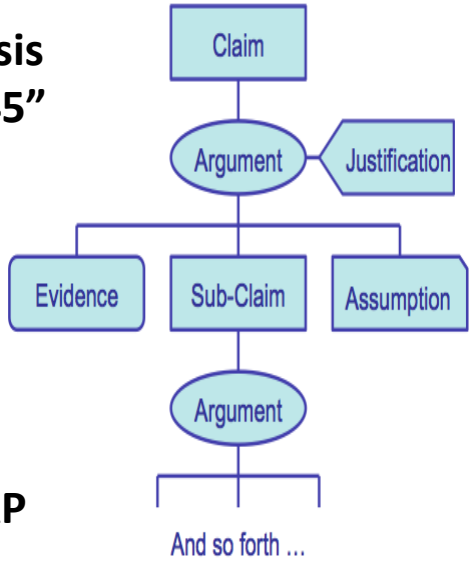
Secretariat: DIN, Germany

DOC TYPE:	NB NWI Proposal for a technical report (TR)
TITLE:	**National Body New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405"**
SOURCE:	INCITS/CS1, National Body of (US)
DATE:	2009-09-30
PROJECT:	**15408 and 18405**
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 27/WG 3 to be held in Redmond (WA, USA) on 2nd – 6th November 2009.
ACTION ID:	ACT
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

Common Criteria v4 CCDB

- **TOE to leverage CAPEC & CWE**
- **ISO/IEC JTC 1/SC 7/WG 3, TR 20004: "Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045"**
- **Also investigating how to leverage ISO/IEC 15026 and OMG's Structured Assurance Case Metamodel (SACM)**



NIAP (U.S.) Evaluation Scheme

- **Above plus**
- **Also investigating how to leverage SCAP**

Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related software system process, people and documentation

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports
Risk Analysis, etc)

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort

Process, People, documentation Evidence

Formalized Specifications

Claims, Arguments and Evidence Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Software system Technical Evidence

Executable Specifications

Software System Artifacts

Hardware Environment

Protection Profiles

IA Controls

CWE-CAPEC

NIST

NIST Special Publications:

SP800-36	CVE
SP800-40	CVE, OVAL
SP800-42	CVE
SP800-44	CVE
SP800-51	CVE
SP800-53a	CVE, OVAL, CWE
SP800-61	CVE, OVAL
SP800-70	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-82	CVE
SP800-86	CVE
SP800-94	CVE
SP800-115	CVE, CCE, CVSS, CWE
SP800-117	CVE, OVAL, CCE, CPE, XCCDF, CVSS
SP800-126	CVE, OVAL, CCE, CPE, XCCDF, CVSS

NIST Interagency Reports:

NISTIR-7007	CVE
NISTIR-7275	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7435	CVE, CVSS, CWE
NISTIR-7511	CVE, OVAL, CCE, CPE, XCCDF, CVSS
NISTIR-7517	CVE
NISTIR-7581	CVE
NISTIR-7628	CVE, CWE

NIST SAMATE
SP 500-267
SP 500-269
SP 500-270

SAMATE Repository Dataset (SRD)

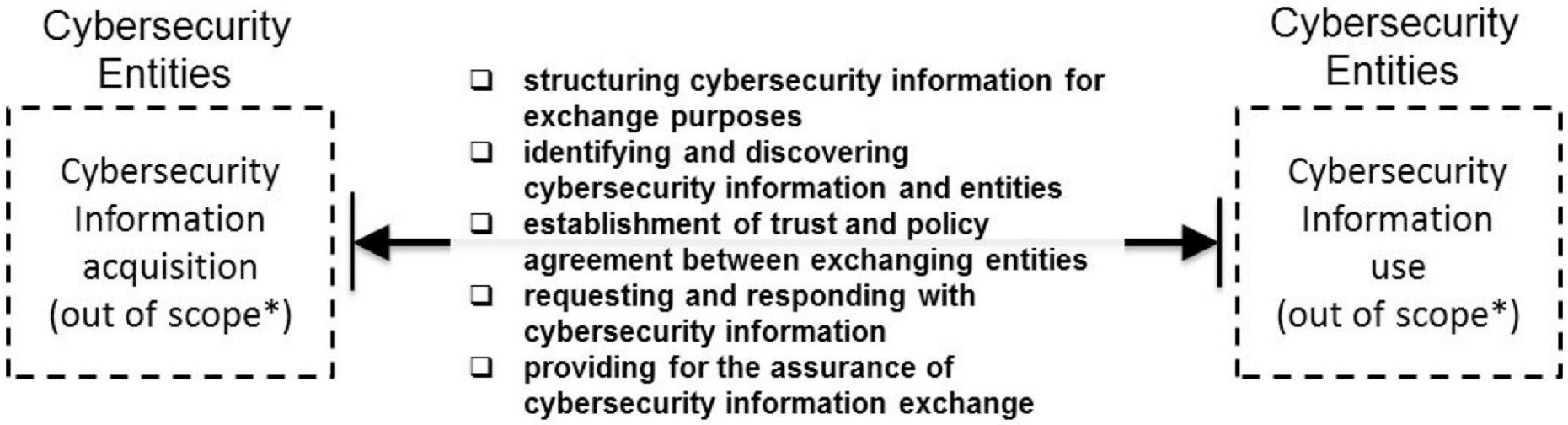
Automated Test Case Generator

NIST SATE
SATE2008
SATE2009
SATE2010

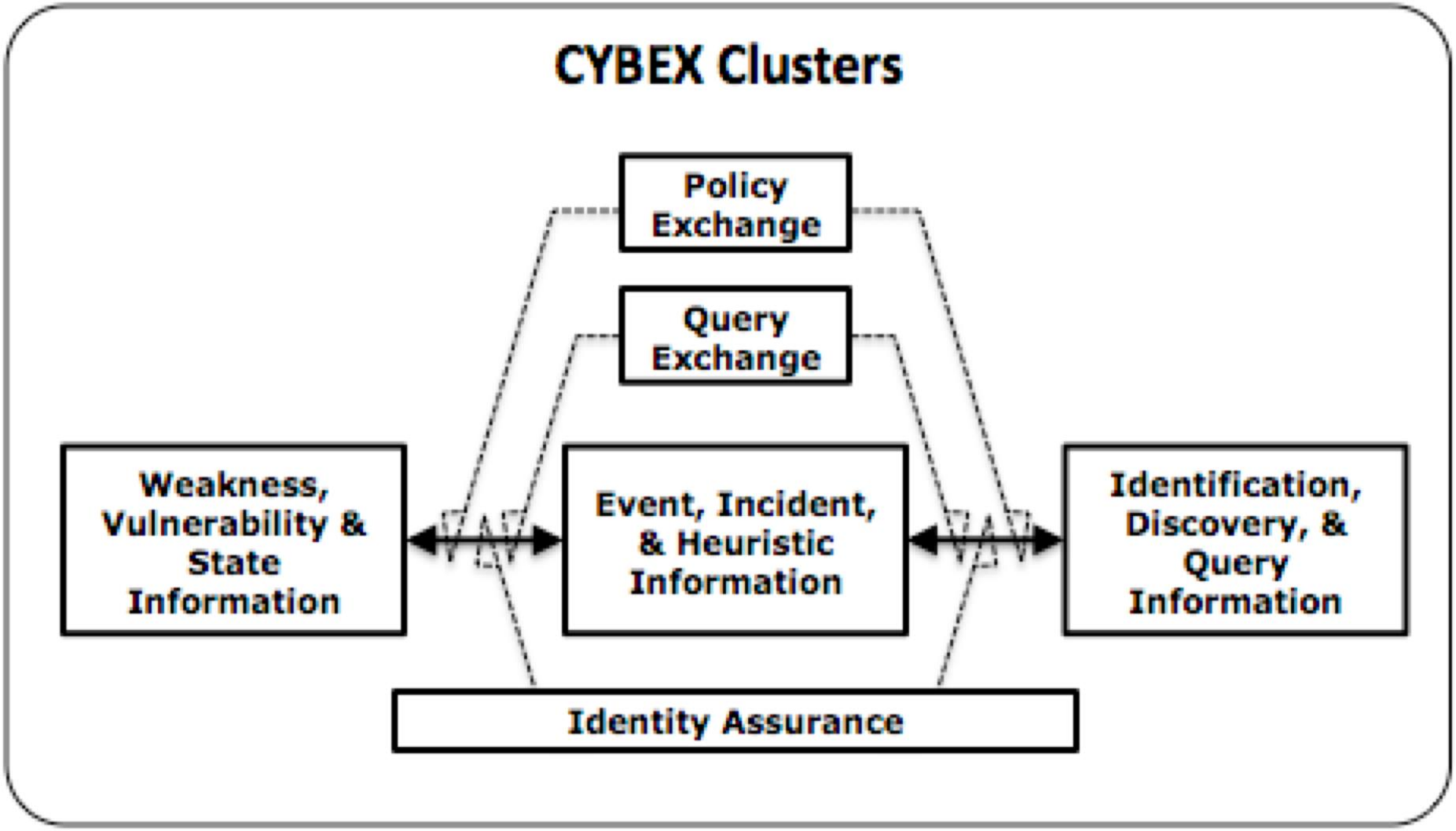
FDCC
USGCB

ITU-T Study Group 17 Question 4

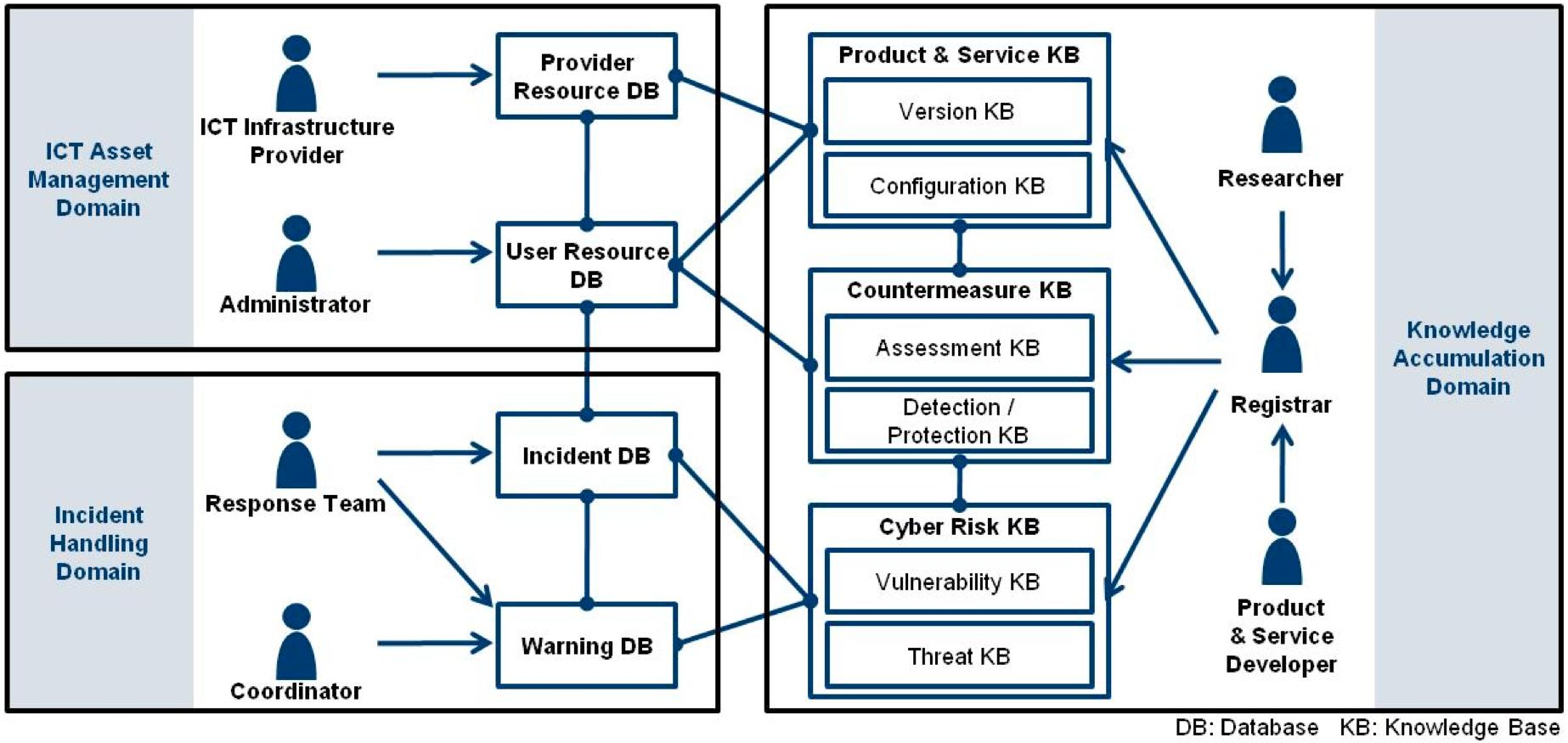
ITU-T Study Group 17 Question 4
The CYBEX Model



* Some specialized cybersecurity information exchange implementations may require application specific frameworks specifying acquisition and use capabilities

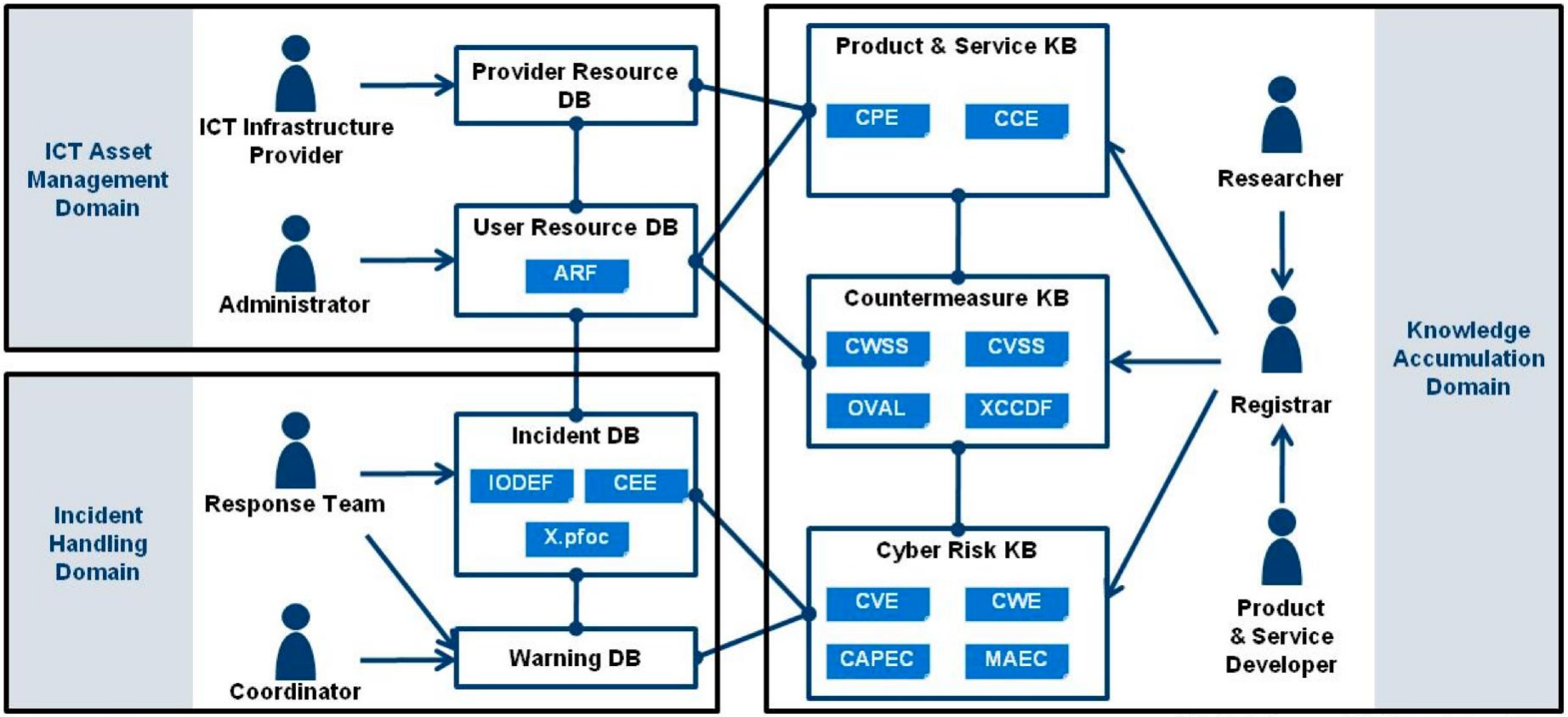

CYBEX Clusters
Policy Exchange
Query Exchange
Weakness, Vulnerability & State Information
Event, Incident, & Heuristic Information
Identification, Discovery, & Query Information
Identity Assurance

CYBEX ontology model



DB: Database KB: Knowledge Base

Detailed view of the CYBEX ontology model with techniques shown



DB: Database KB: Knowledge Base

ITU-T Study Group 17 Question 4: Adopting the Information Security Community's Efforts

XXX is one of a class of ITU-T Recommendations that comes from a large, existing, global development and user community that has written and evolved an open specification that is made available to the ITU-T for adoption with agreement that any changes or updates to the specification will be done in a manner that ensures full technical equivalency and compatibility will be maintained, that discussions about changes and enhancements will be done through the original user community processes, and includes explicit reference to the corresponding specific version maintained by the user community. Thus, at the time of initial adoption of Rec. **X.XXXX**, a due diligence verification and statement of equivalency will occur; and as changes are effected among the user community, timely reflection of those changes will be incorporated in subsequent versions of the Recommendation through continued collaboration.

Status of ITU-T Recommendations

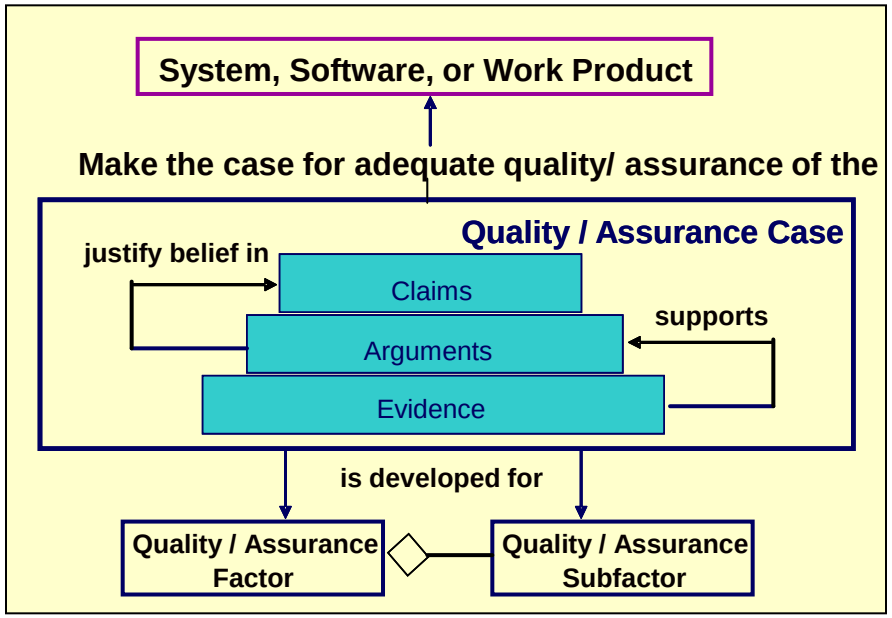
x-series	Title	ITU-T Status	Planned Determination
x.1500	Cybersecurity Information Exchange (CYBEX) Techniques	Final	Dec 2010
x.1520	Common Vulnerabilities and Exposures	Final	Dec 2010
x.1521	Common Vulnerability Scoring System	Final	Dec 2010
x.cwe	Common Weakness Enumeration	Draft	Aug 2011
x.oval	Open Vulnerability and Assessment Language	Draft	Aug 2011
x.cce	Common Configuration Enumeration	Draft	Aug 2011
x.capec	Common Attack Pattern Enumeration and Classification	Draft	Feb 2012
x.maec	Malware Attribute Enumeration and Classification	Draft	2012
x.cwss	Common Weakness Scoring System	Draft	2012
x.cee	Common Event Expression	Draft	2012
x.cpe	Common Platform Enumeration	Draft	2012
x.arf	Asset Reporting Format	Draft	2012
x.xccdf	Extensible Configuration Checklist Description Format	Draft	2012

Bob Martin, 23 February 2011

ISO/IEC – JTC1/SC 7, SC 22, and SC27

ISO/IEC JTC1 SC7 15026 Assurance Case

- **Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.**
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources



- **Sub-parts**
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards & regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard / threat
  - Operational & support assumptions

Attributes

- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages

ISO/IEC JTC1 SC22 WG23, TR 24772, Programming Language Vulnerabilities

The Problem:

- Any programming language has constructs that are imperfectly defined, implementation dependent or difficult to use correctly.
- As a result, software programs sometimes execute differently than intended by the writer.
- In some cases, these weaknesses can be exploited by hostile parties, or can lead to failure in anticipated environments.
  - Can compromise safety, security, privacy, dependability or other critical properties.
  - A vulnerability in any program can be used as a springboard to make additional attacks on other programs.

ISO/IEC JTC1 SC22 WG23, TR 24772, Programming Language Vulnerabilities

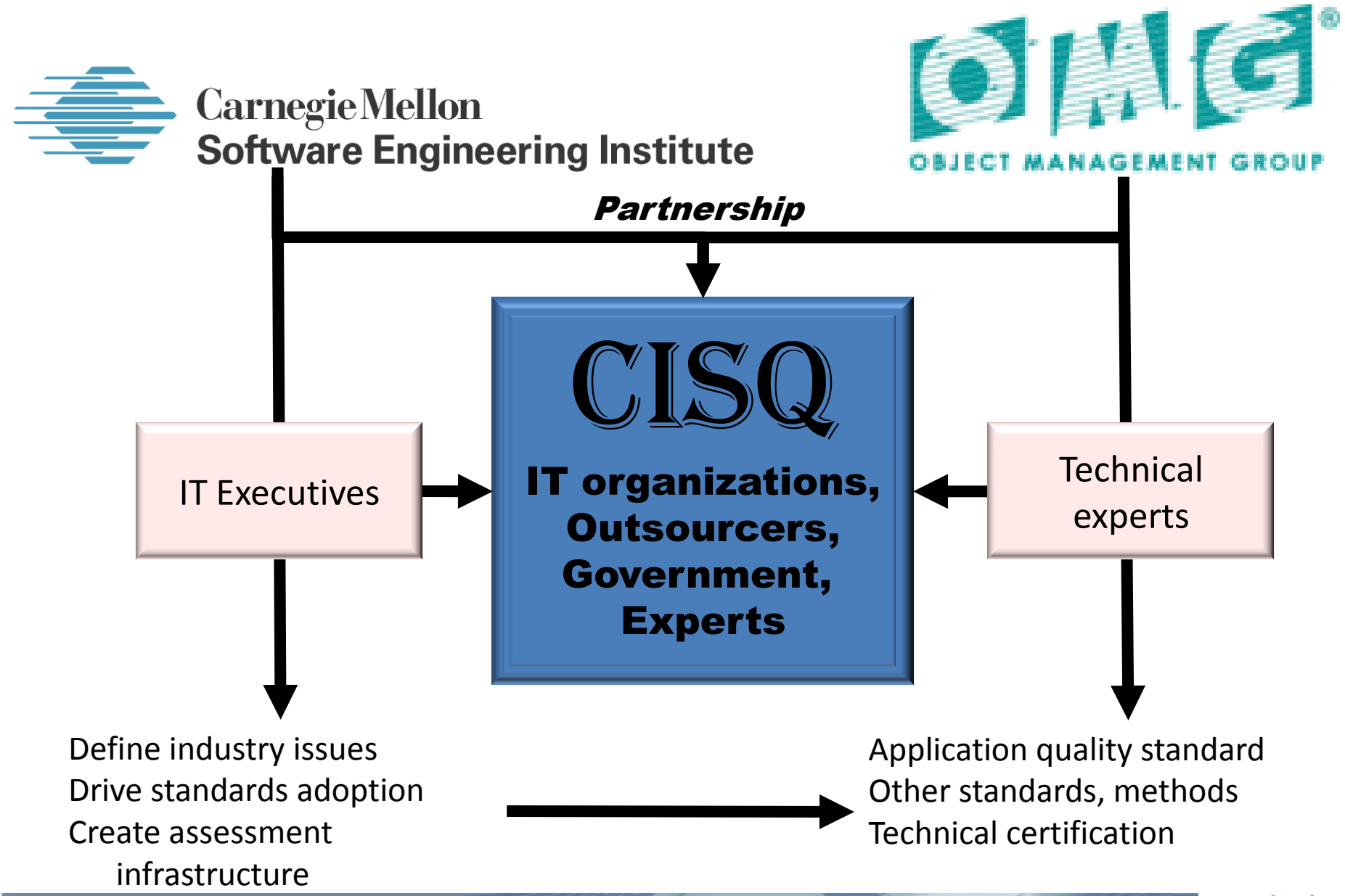
- A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities.
- Cross-referenced to CWE.
- Each discussion includes…
  - Description of the mechanism of failure
  - Recommendations for programmers: How to avoid or mitigate the problem.
  - Recommendations for standardizers: How to improve programming language specifications.
- First edition published in late 2010.
- Second edition will add annexes specific to particular programming languages.

ISO/IEC JTC1 SC22 WG23 Participants

- National Bodies
  - Canada
  - Germany
  - Italy
  - Japan
  - France
  - United Kingdom
  - USA
- Other Groups
  - RT/SC Java
  - MISRA C/C++
  - CERT

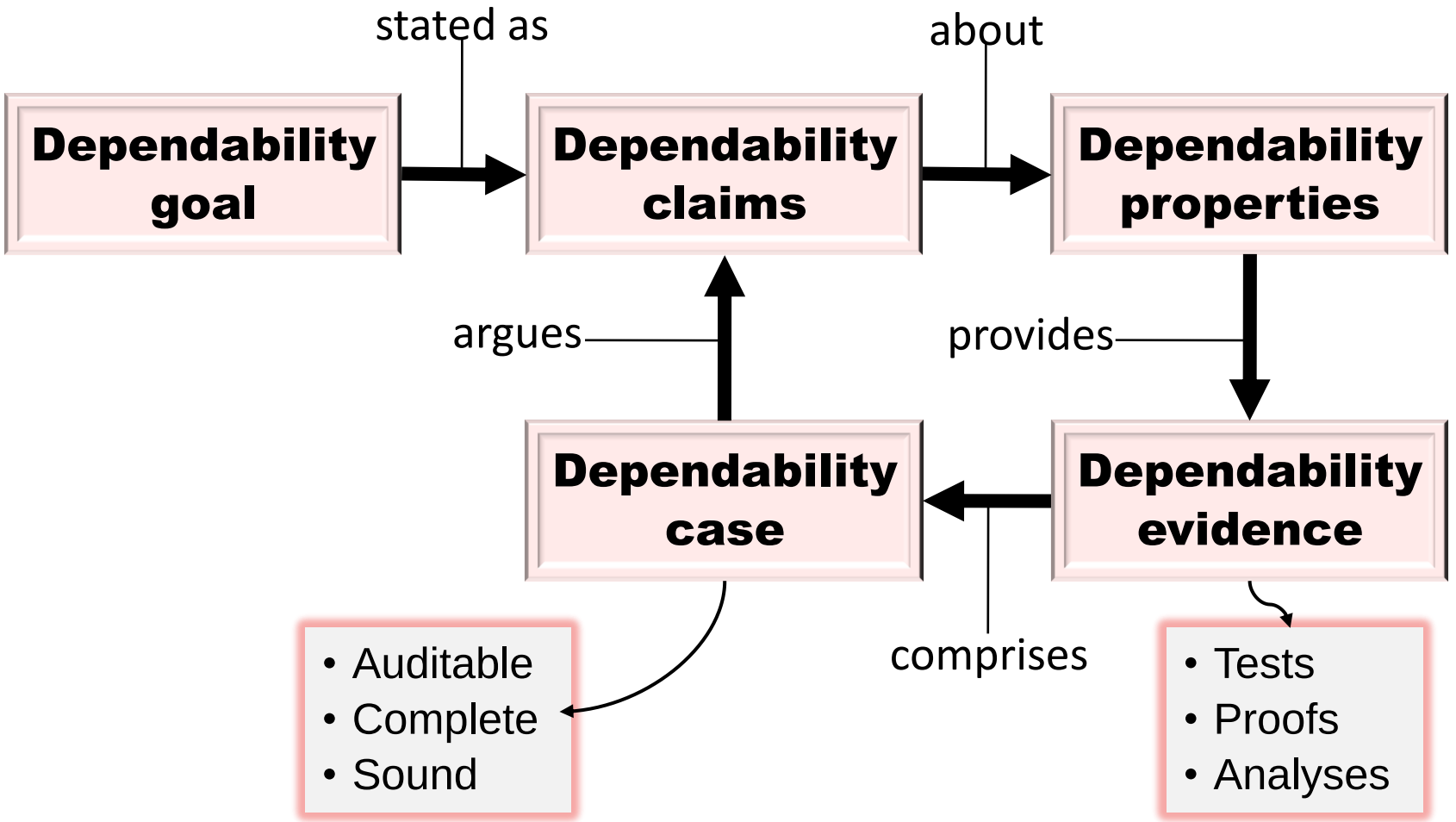
- Language Standards Groups
  - SC 22/WG 9
  - SC 22/WG14
  - SC 22/WG 5, INCITS J3 (Fortran)
  - SC 22/WG 4, INCITS J4 (Cobol)
  - MDC (Mumps)
  - ECMA (C#, C++CLI)

What Is CISQ?

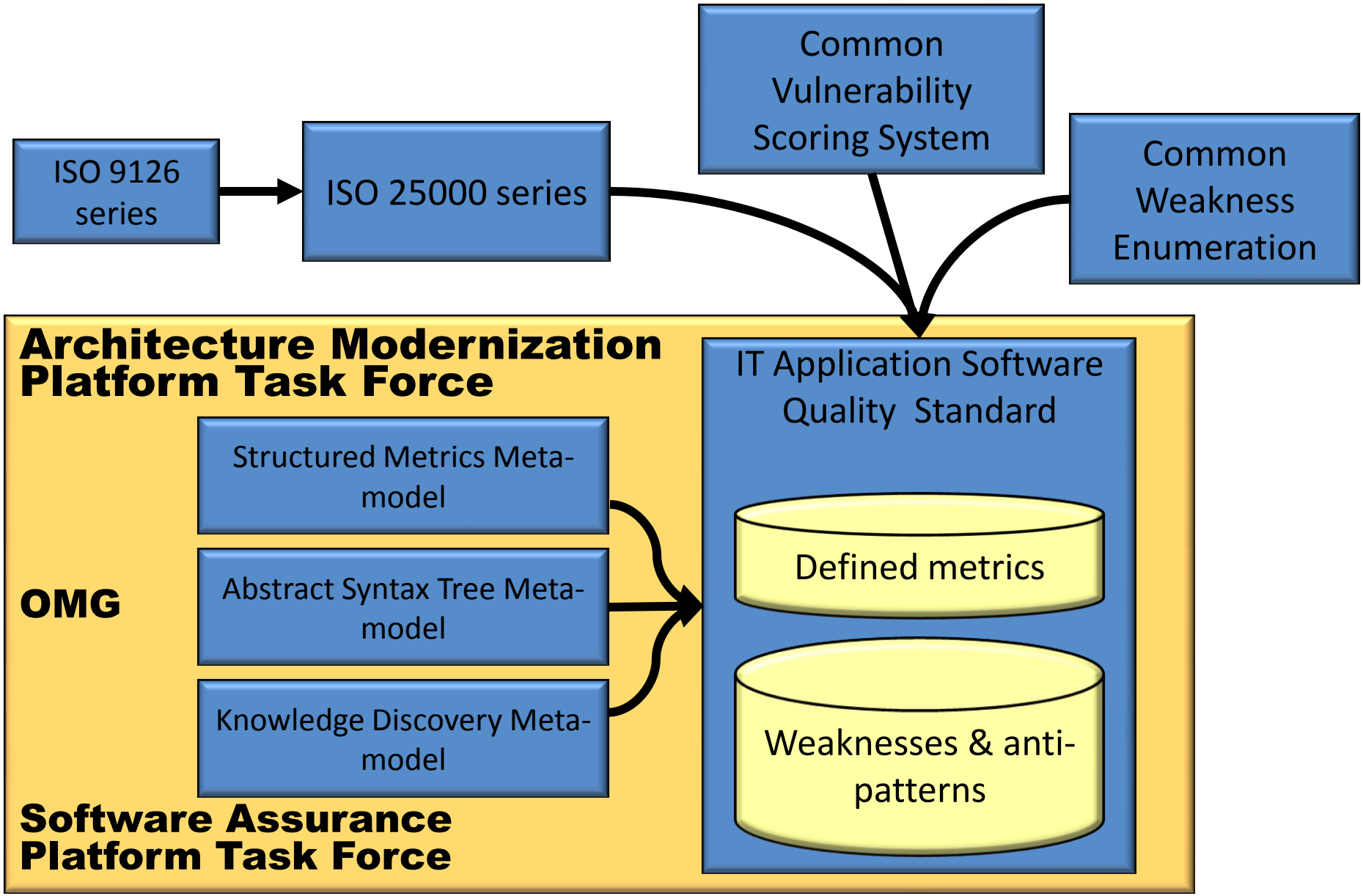

Carnegie Mellon
Software Engineering Institute
OMG
OBJECT MANAGEMENT GROUP
Partnership
CISQ
IT organizations, Outsourcers, Government, Experts
IT Executives
Technical experts
Define industry issues
Drive standards adoption
Create assessment infrastructure
Application quality standard
Other standards, methods
Technical certification

Presenting Dependability Cases

Objective — **Provide direct evidence that a system satisfies its dependability requirements**



CISQ Standards Infrastructure



Questions?

ramartin@mitre.org