

Engineering Improvement in Software Assurance: A Landscape Framework

Lisa Brownsword (presenter)
Carol C. Woody, PhD
Christopher J. Alberts
Andrew P. Moore



Agenda

Assurance Terminology

Problem Scope

Modeling Framework Overview

Selected Elements of the Framework Pilot

Summary and Next Steps



Assurance

System assurance

- The justified confidence that a system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle*

Software assurance

- Software's contribution to system and system of systems (SoS) assurance
 - Software assurance in the context of a system's and SoS mission and use

Justified confidence: rational basis for deciding about SoS readiness for use

Functions as intended: involves user expectations, which change over time

Environment of use

- Actual environment of use (not just the expected environment of use)
- Means evaluating robustness against *unexpected* use, threats, and changes in the environment

* Engineering for System Assurance, NDIA System Assurance Committee, 2008, www.acq.osd.mil/sse/pg/guidance.html



Problem Scope

Numerous assurance solutions (i.e., technologies, policies, and practices) are available

- A large number of organizations produce, fund, or use these assurance solutions
- How these assurance solutions contribute to operational assurance is often unclear

Operational environments are plagued with undiscovered defects and escalating numbers of known vulnerabilities

- Where should resources be invested to gain the most benefit?
- Where are the critical gaps in available assurance solutions?
- What additional assurance solutions are needed?
- Are the incentives for routinely applying assurance solutions effective?



A Solution Approach

Goal – longer-term

- Identify gaps, barriers, and incentives to the formation, adoption, and application of assurance solutions (i.e., technologies, policies, practices) to improve operational assurance
- Exploit this knowledge to accelerate the formation, adoption, and application of appropriate assurance solutions

Near-term approach

- Build a modeling framework that
 - Characterizes the current portfolio of organizations working in assurance, available assurance solutions, and how they work together to improve operational assurance
 - Characterizes the gaps, barriers, and incentives related to the adoption and application in operational environments of assurance solutions
- Leverage (or adapt) existing modeling and analysis methods



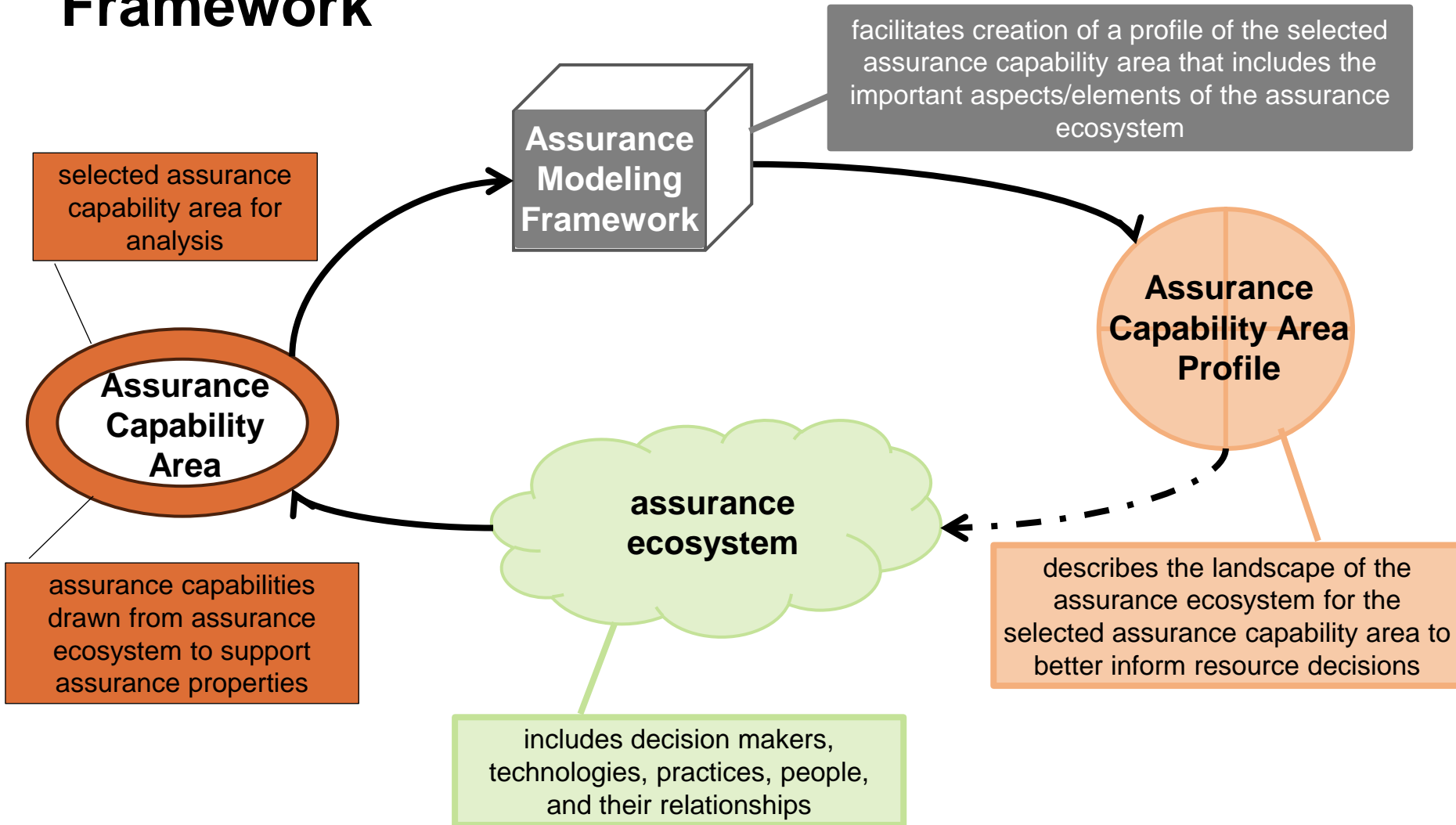
Where might we start?

Key Information for a Modeling Framework to Address

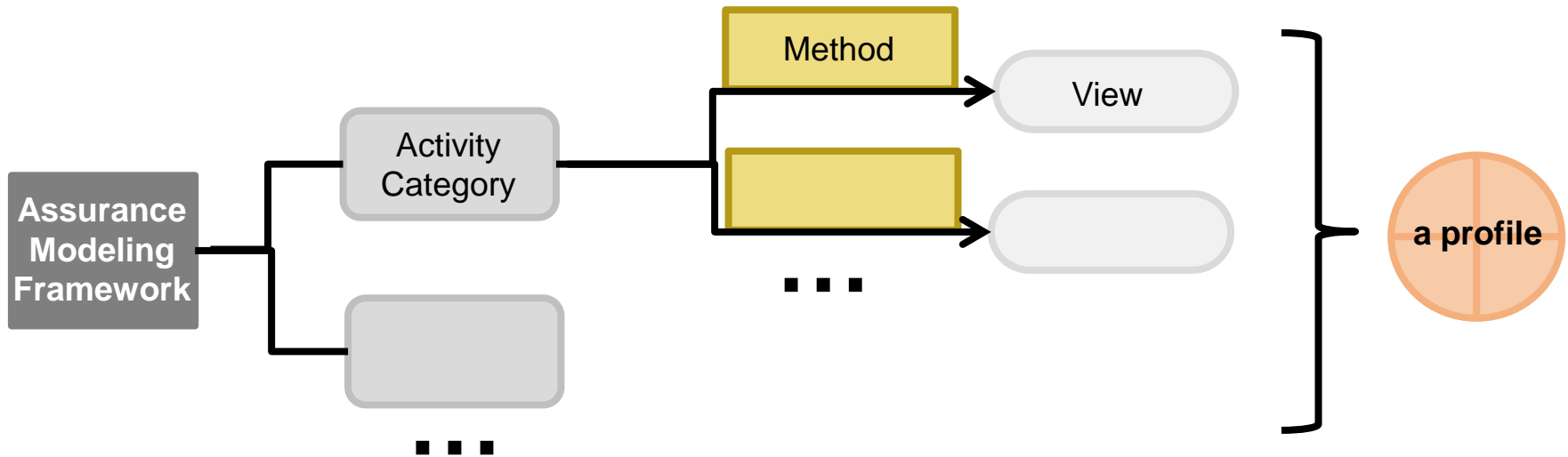
- 1 How is software assurance value defined for a selected context?
- 2 Who/what are the participating organizations and assurance solutions?
- 3 What are the elements of value exchanged among participants?
- 4 How do participating organizations and assurance solutions work together to achieve operational assurance?
- 5 What are the drivers and motivations of participating organizations?
- 6 What are the critical usage scenarios and behaviors among the participating organizations and assurance solutions?
- 7 What are the adoption and operational usage mechanisms used for assurance solutions?
- 8 How are the adoption and operational usage mechanisms aligned with organizational context and need?
- 9 What is the impact of future trends and events on participating organizations and assurance solutions?
- 10 What patterns of possible inefficiencies can be identified?
- 11 What are candidates for improvements? What could be the impact, if implemented?



Conceptual Context of Assurance Modeling Framework



Structure of Assurance Modeling Framework



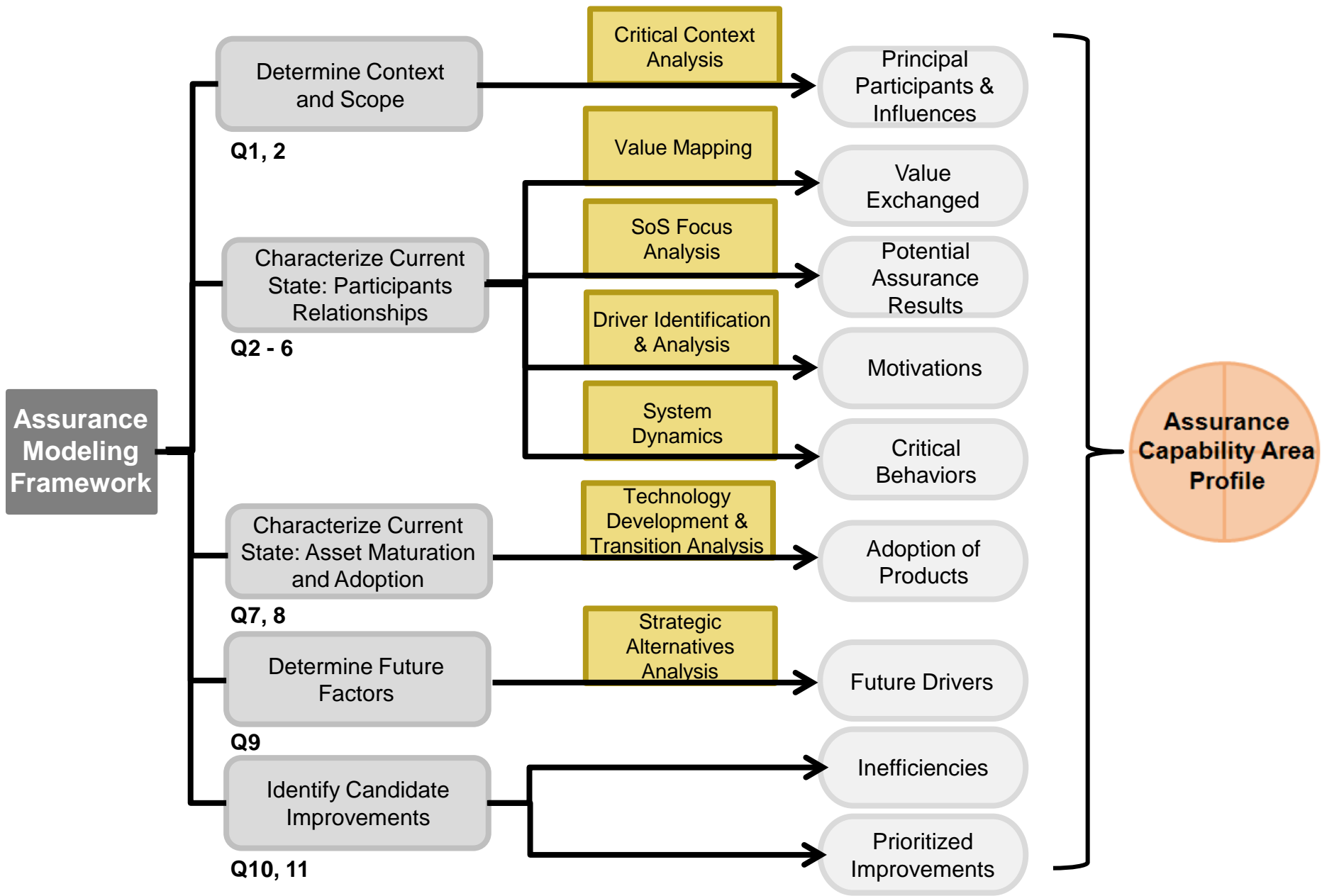
Our modeling framework is comprised of multiple *categories of activities* necessary to produce an assurance capability area profile

Each activity category focuses on developing insights on one or more of the framework information questions and produces one or more *views*

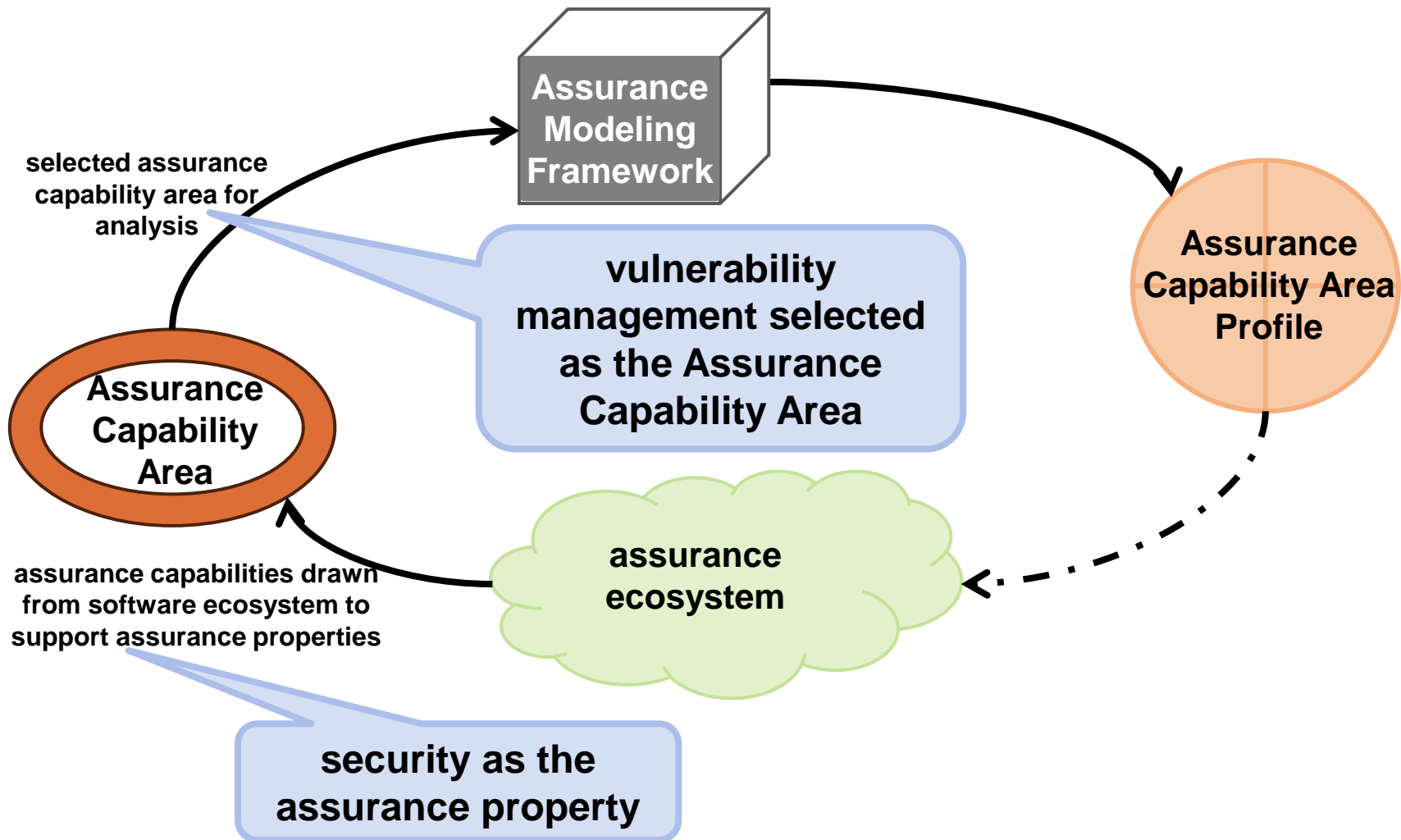
Each view is formed using one or more *methods*

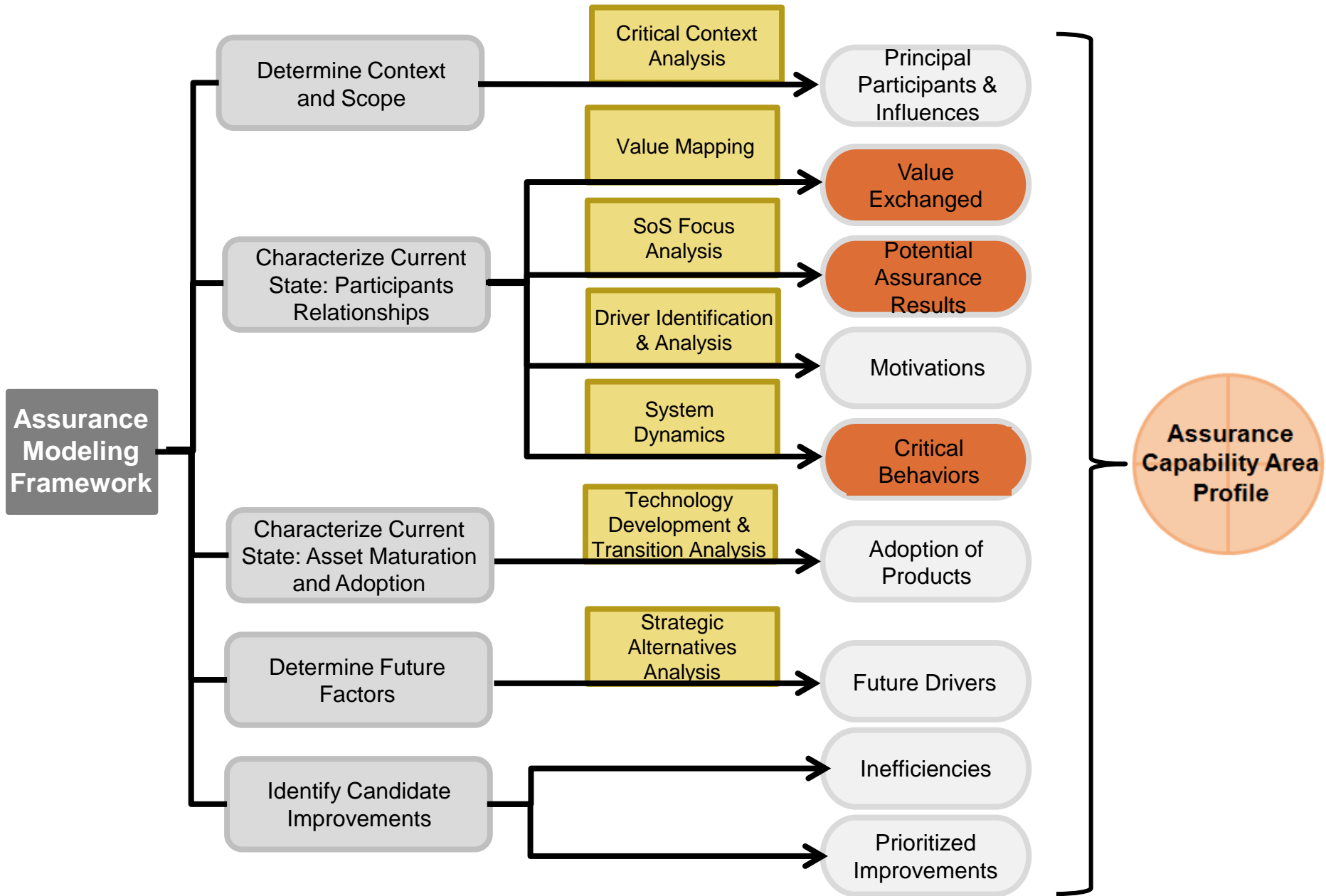
A *profile* is a set of views that collectively describe an assurance landscape





Pilot Use of the Assurance Modeling Framework





View: Value Exchanged (Q2, 3, 4)

Method: Value Mapping



- Shows static relationships among principal participants (organizations and assurance solutions)
- Shows primary elements of value exchanged between two participants

Selected insights



- One organization or technology by itself does not mean a great deal; its relationship to other organizations and technologies has meaning
 - An organization may play several roles in the assurance ecosystem
- Values identified in value exchanges may have only an indirect effect on operational assurance and is often difficult to determine
- The models provide an effective way for assurance solution owners to describe and better understand the key relationships associated with their solution



Symbols







-  Participant A participant (e.g., organization or technology) in a value exchange
-  Data source for public information with multiple contributors

Line Style

-  Dashed arrow Value is pulled by destination organization.
-  Solid arrow Value is pushed from source organization.

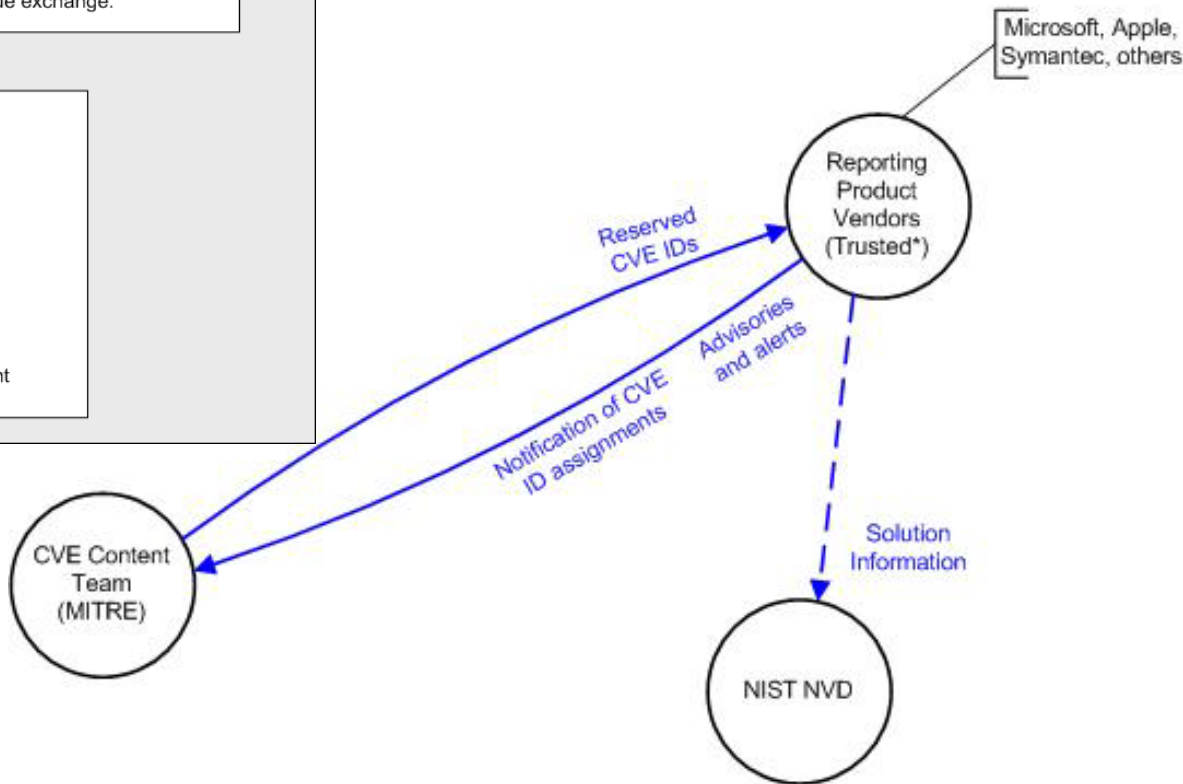
Note: The direction of the arrow shows the flow of the value exchange.

Line Colors

-  Green Funding
-  Blue Product
-  Brown Service
-  Gray Governance
-  Red Compliance
-  Orange Endorsement

Sample CVE Value Map -1

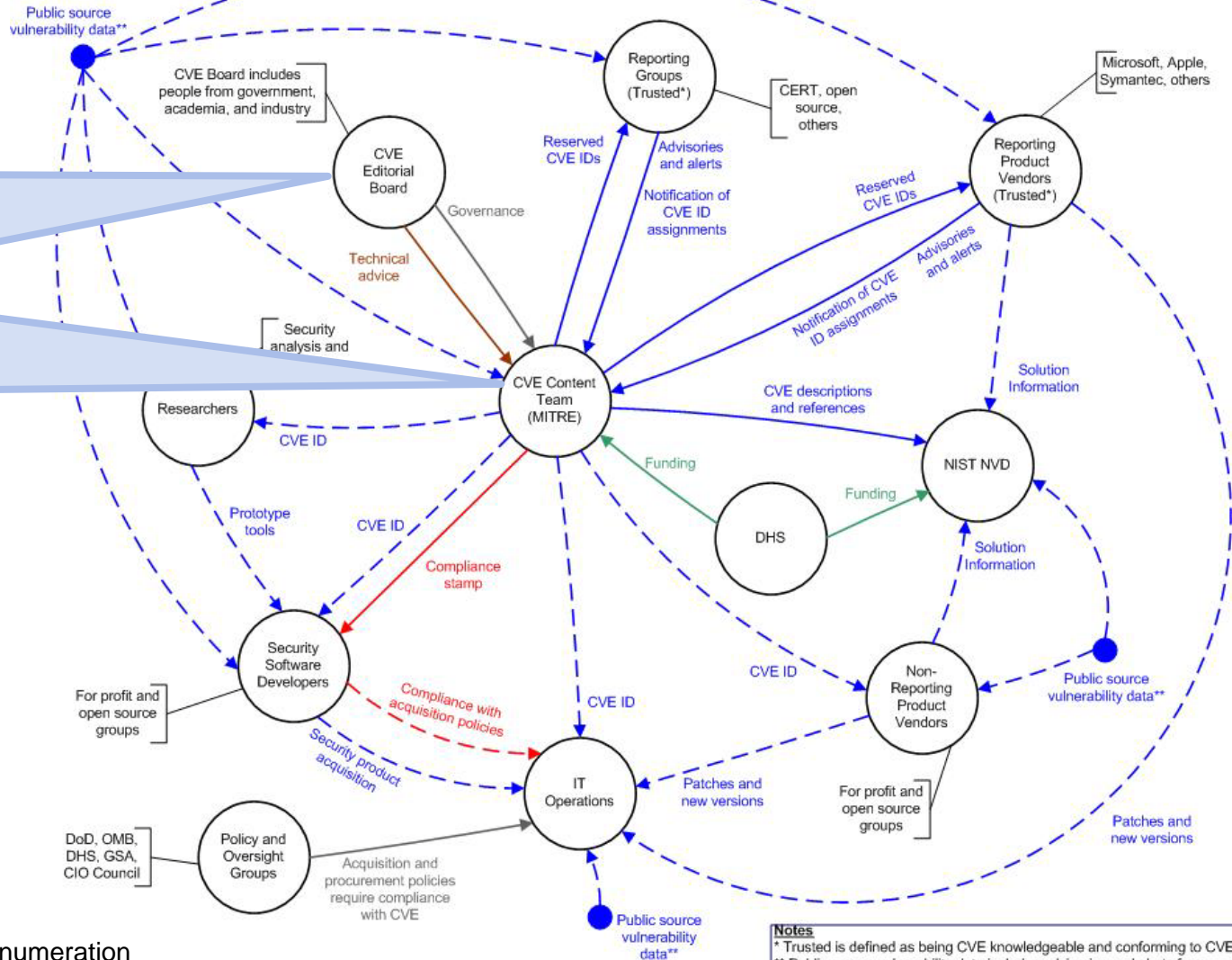
Partial CVE Diagram – Notation Example



Sample CVE Value Map -2

CVE Diagram

An organization may play multiple roles with different values exchanged



Notes
 * Trusted is defined as being CVE knowledgeable and conforming to CVE guidelines.
 ** Public source vulnerability data includes advisories and alerts from Reporting Groups and Reporting Product Vendors.

CVE – Common Vulnerability Enumeration
 NVD – National Vulnerability Database



View: Potential Assurance Results (Q2, 4)

Method: SoS Focus Analysis

- Produces a model for alignment of services between suppliers of assurance solutions to what operational users do to achieve operational assurance
- Oriented to defining collaborations within complex, socio-technical systems (of systems) domains

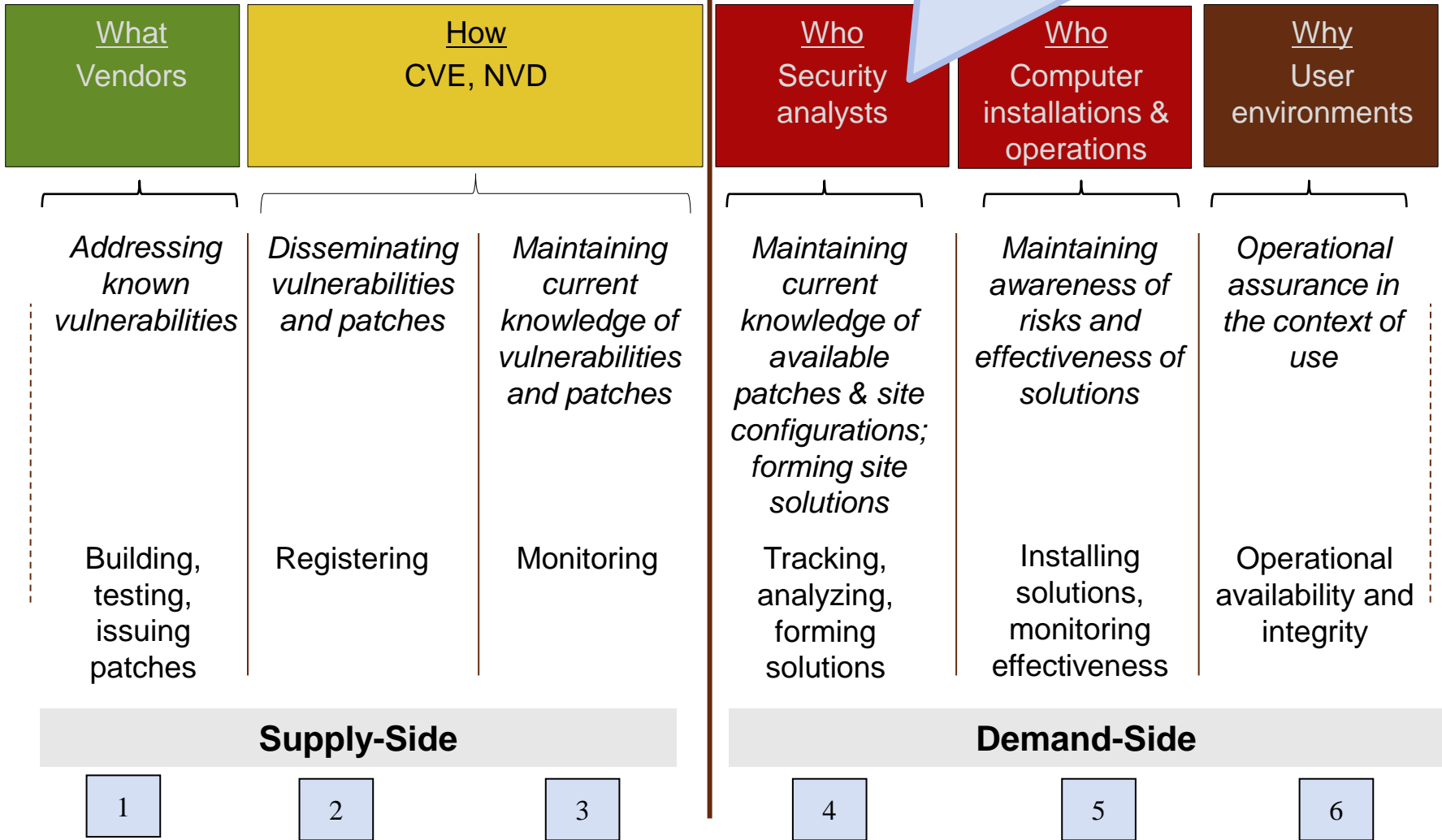
Selected insights

- The effect an assurance solution has on achieving operational assurance is often not direct
 - It is a network of relationships among organizations and assurance solutions that must be understood within their operational context
- The models surface potential areas of inefficiencies for further analysis



SoS Focus Analysis with CVE

Potential inefficiencies:
 - where tacit knowledge is held
 - where people manually synthesize significant information from multiple sources



View: Critical Behaviors (Q6)

Method: System Dynamics

- Produces a model for analyzing critical behaviors within complex socio-technical system of system domains
- Identifies primary positive and negative feedback loops driving critical behaviors

Selected insights

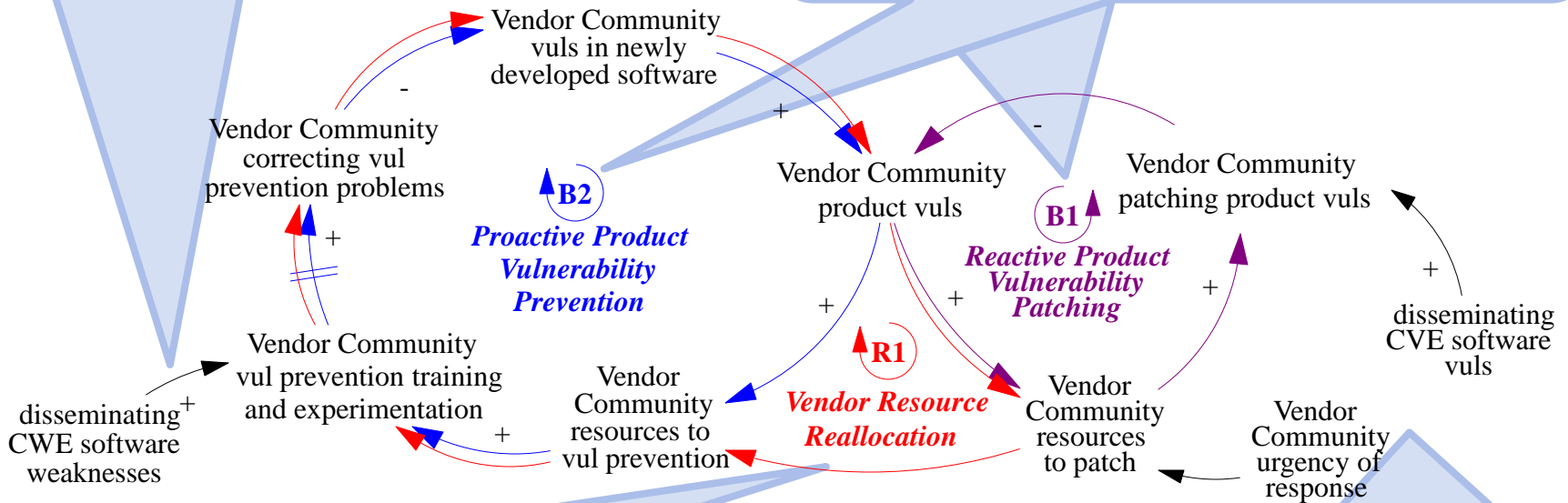
- There is a tension in the vendor community between resources for proactive software vulnerability prevention practices and reactive patch generation and release practices
 - Urgency of response has historically promoted reactive practices
 - CVE-induced market pressures are beginning to promote proactive practices
- The models provide a structured way to approach discussions among technology representatives and other affected stakeholders



Sample System Dynamics Model

3. The proactive approach focuses on a strategy of vulnerability prevention based on applying CWE information within the vendor community to developed software that prevents vulnerabilities.

1. Vendors must decide how to split resources between reactive and proactive responses to product vulnerabilities to balance the need for an immediate response with the need for a proactive solution that prevents product vulnerabilities.



4. If vendors feel the need to devote more resources to vulnerability patching and less to vulnerability prevention, then this leads to a downward spiral of increasingly vulnerable products and ever increasing assurance problems.

2. The reactive approach patches product vulnerabilities based on CVE information. The development of patches is prioritized based, in part, on the impact a given vulnerability is having on the operational community.



Summary

Assurance modeling framework lays important groundwork by providing a multi-dimensional approach to

- Better understand relationships between organizations and assurance solutions and how these relationships contribute to operational assurance
- Begin identifying potential areas of inefficiencies across a spectrum of technical and organizational areas

Status of SoS software assurance modeling framework project

- Completed initial version of the assurance modeling framework and validated it through the pilot on vulnerability management as a selected assurance capability area
- Finishing up a report on the modeling framework and its pilot use



Next Steps

- Expand modeling of future trends and technology formation and adoption
- Review the behavioral system dynamics models with community representatives
- Review usage scenarios of the pilot profile with community representatives
- Expand the use of the framework to another aspect of software assurance



Contact Information

Lisa Brownsword

Senior Member, Technical Staff
Research, Technology, and System
Solutions (RTSS) Program

+1 703-908-8203

llb@sei.cmu.edu

Christopher J. Alberts

Senior Member, Technical Staff
Acquisition Support Program
(ASP)

+1 412-268-3045

cja@sei.cmu.edu

Carol C. Woody, PhD.

Senior Member, Technical Staff
Networked Systems Survivability
(NSS) Program

+1 412-268-9137

cwoody@cert.org

Andrew P. Moore

Senior Member, Technical Staff
Networked Systems Survivability
(NSS) Program

+1 412-268-5465

apm@cert.org



NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

