Engineering Improvement in Software Assurance: A Landscape Framework

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

Agenda

Terminology and Problem Scope

Modeling Framework Overview

Selected Elements of the Framework Pilot

Summary and Next Steps

Assurance

System assurance

- 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

- Implications on system of systems (SoS) assurance
- Importance of context of a system's and SoS mission and use

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

Context of use: actual environment of use (not just the expected environment of use)

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

Problem Scope

Assurance encompasses many *properties*: e.g., safety, security, reliability, etc.

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

Framing the problem space

- 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

- Identify gaps, barriers, and incentives to the formation, adoption, and application of assurance solutions to improve operational assurance
- Exploit this knowledge to incentivize the formation and application of appropriate assurance solutions

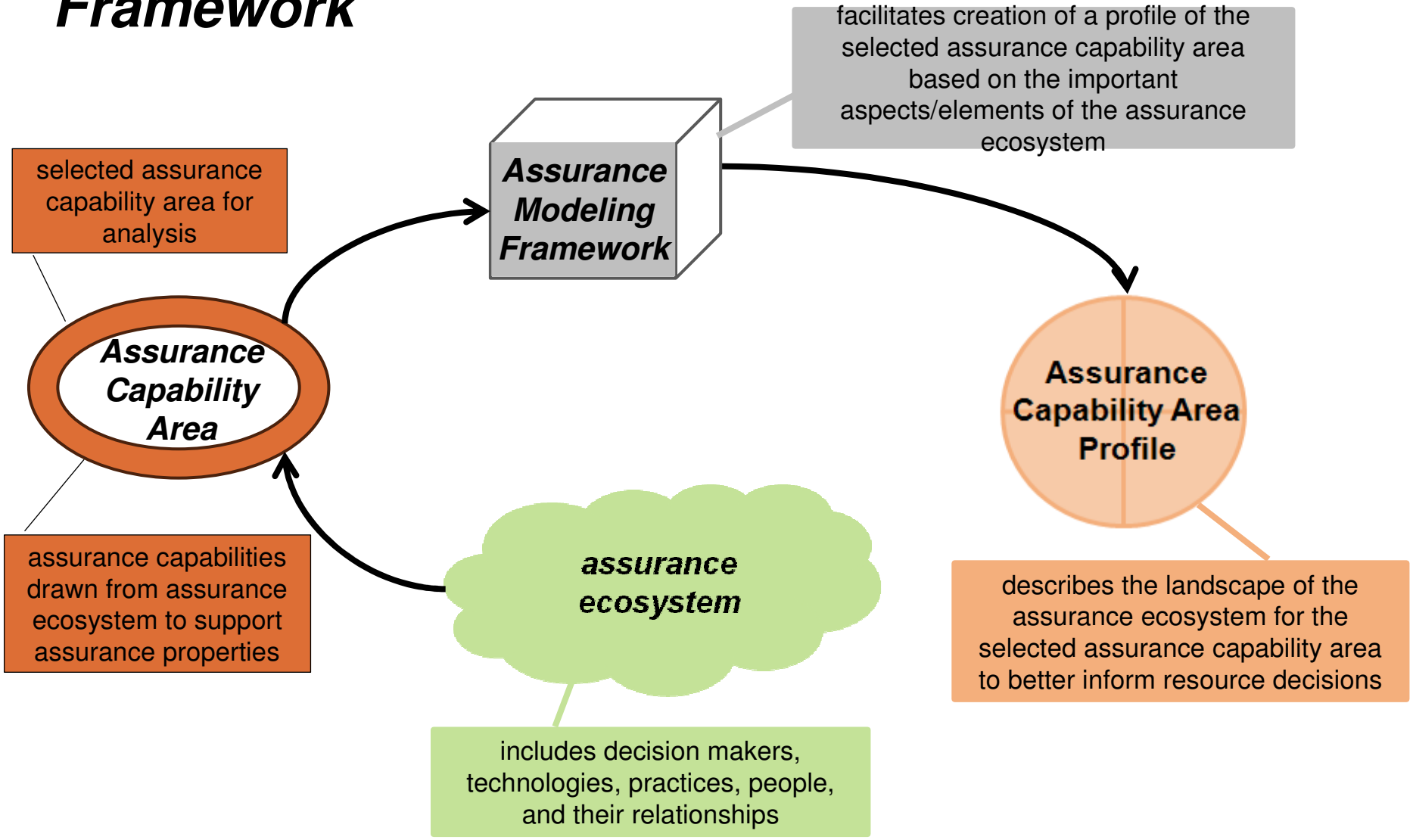
Near-term approach

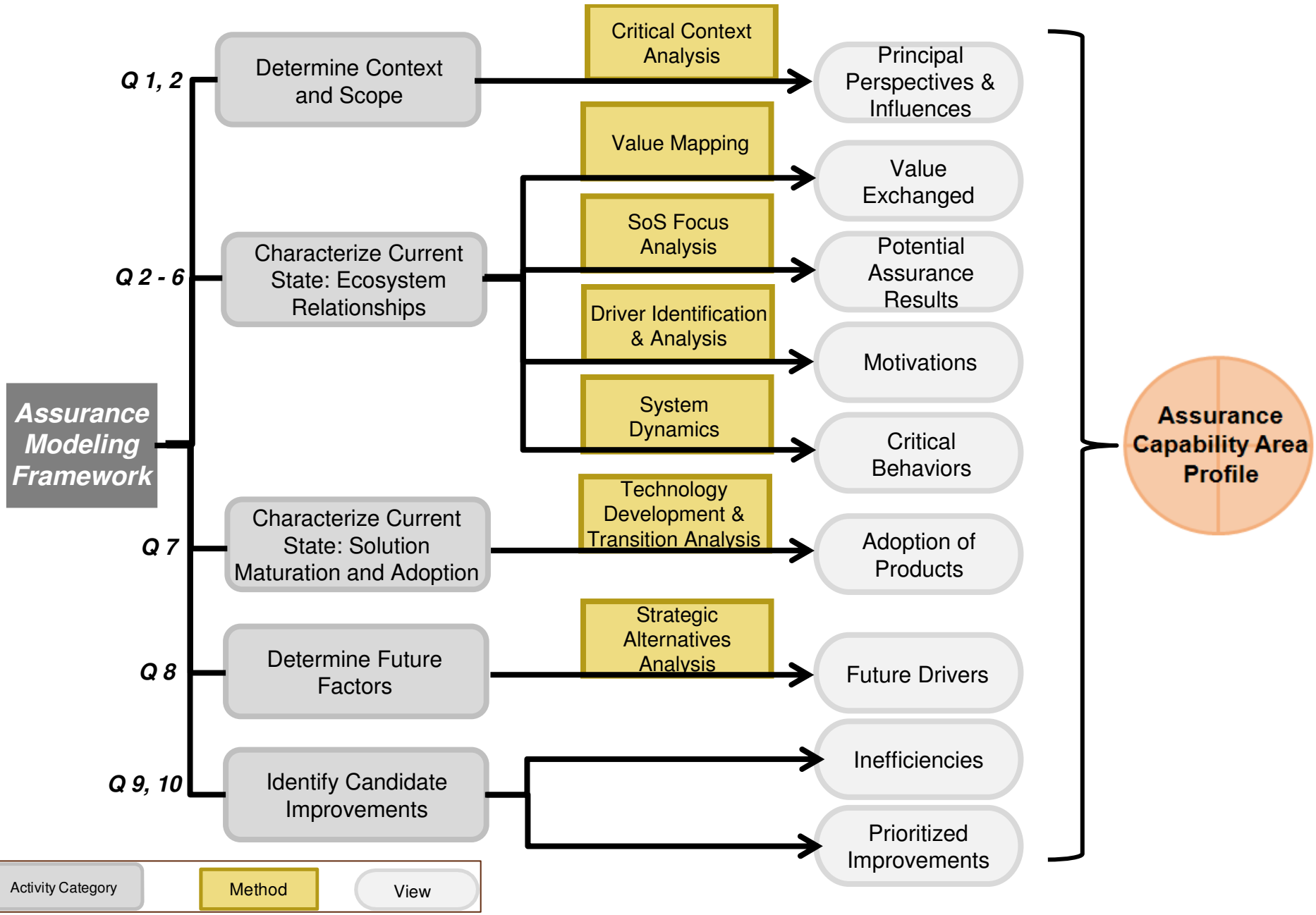
- Build a modeling framework
  - Characterizes the current portfolio of organizations working in assurance, available assurance solutions, and how they work together to improve operational assurance
  - Characterizes the gaps, barriers, and incentives related to the adoption and application in operational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

Where might we start?

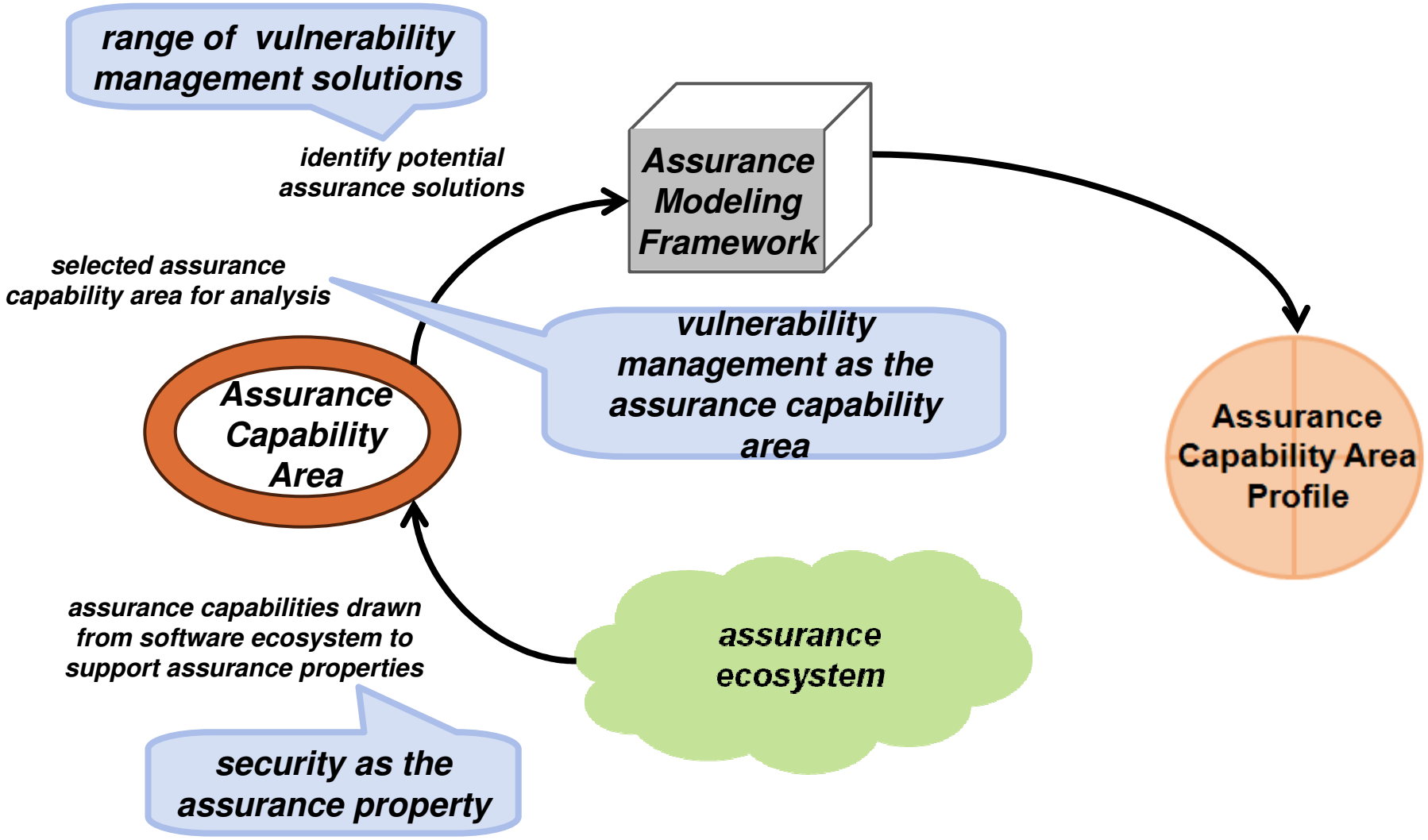
	Key Questions the Framework is Designed to Answer
1	How is software assurance value defined for a selected context?
2	Who/what are the participating organizations and assurance solutions?
3	What are the elements of value exchanged among participating organizations and assurance solutions?
4	How do participating 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? How are they aligned with organizational contexts and needs?
8	What is the impact of future trends and events on participating organizations and assurance solutions?
9	What patterns of possible inefficiencies affecting the formation, adoption, and usage of assurance solutions can be identified?
10	What are candidates for improvements? What could be the impact, if implemented?

Conceptual Context of Assurance Modeling Framework

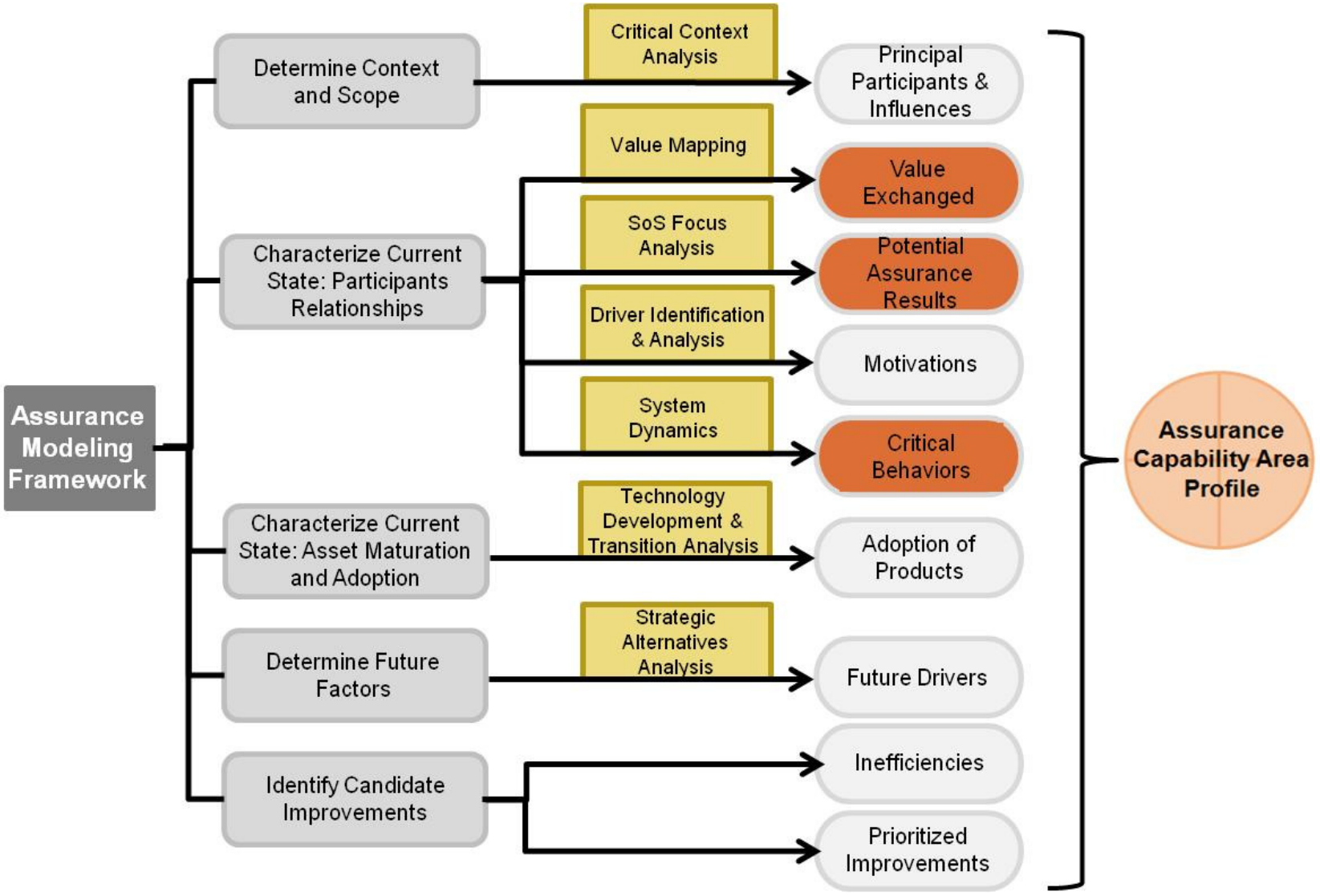




Pilot Use of the Assurance Modeling Framework



Selected Views for Discussion



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 solution by itself does not mean a great deal; its relationship to other organizations and solutions 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 representatives to discover and understand key relationships
- Models evolve through interactions and feedback with solution representatives

Sample CVE® Value Map -1

Legend

Symbols

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

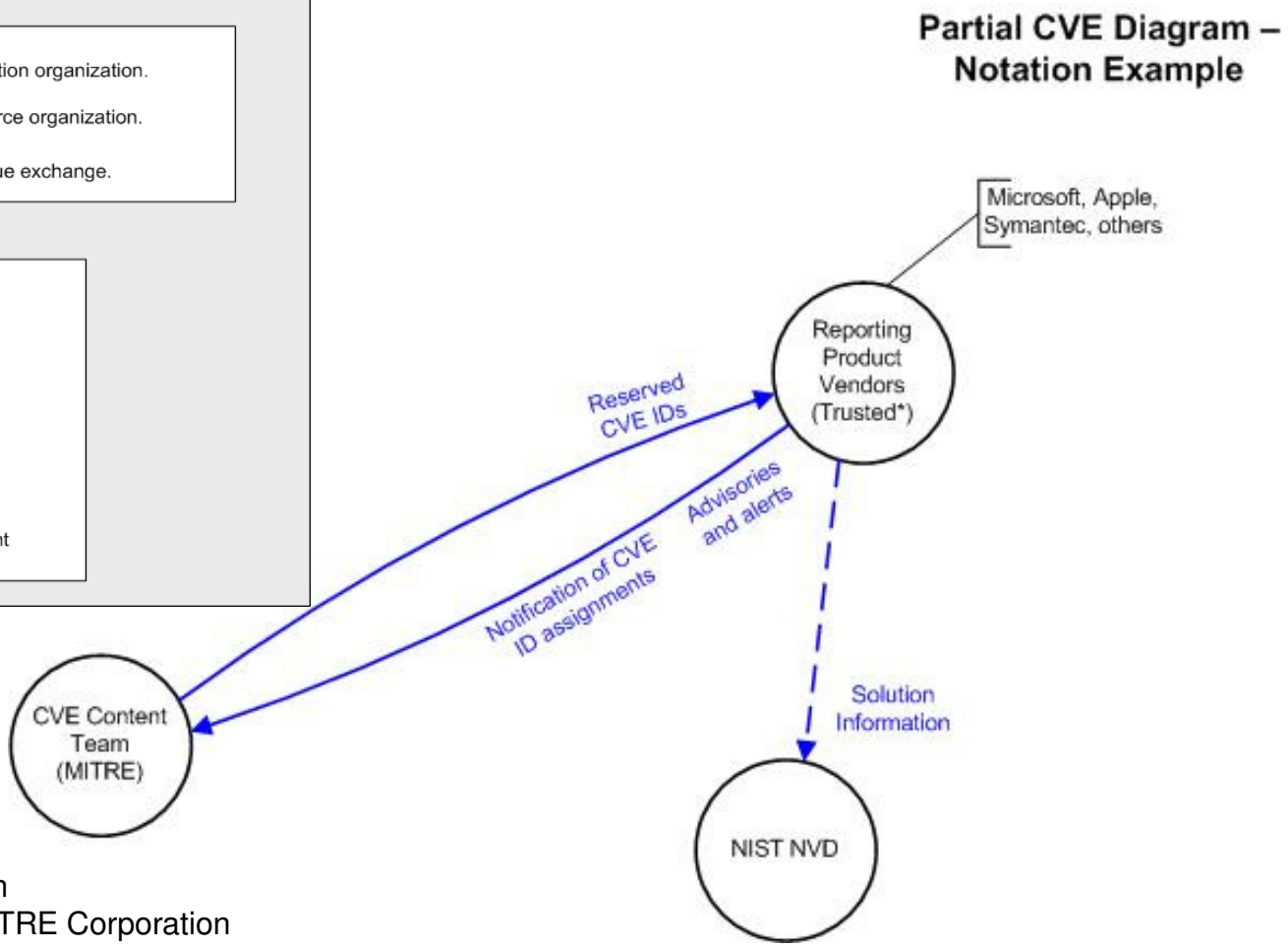
Line Style

– – – →	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

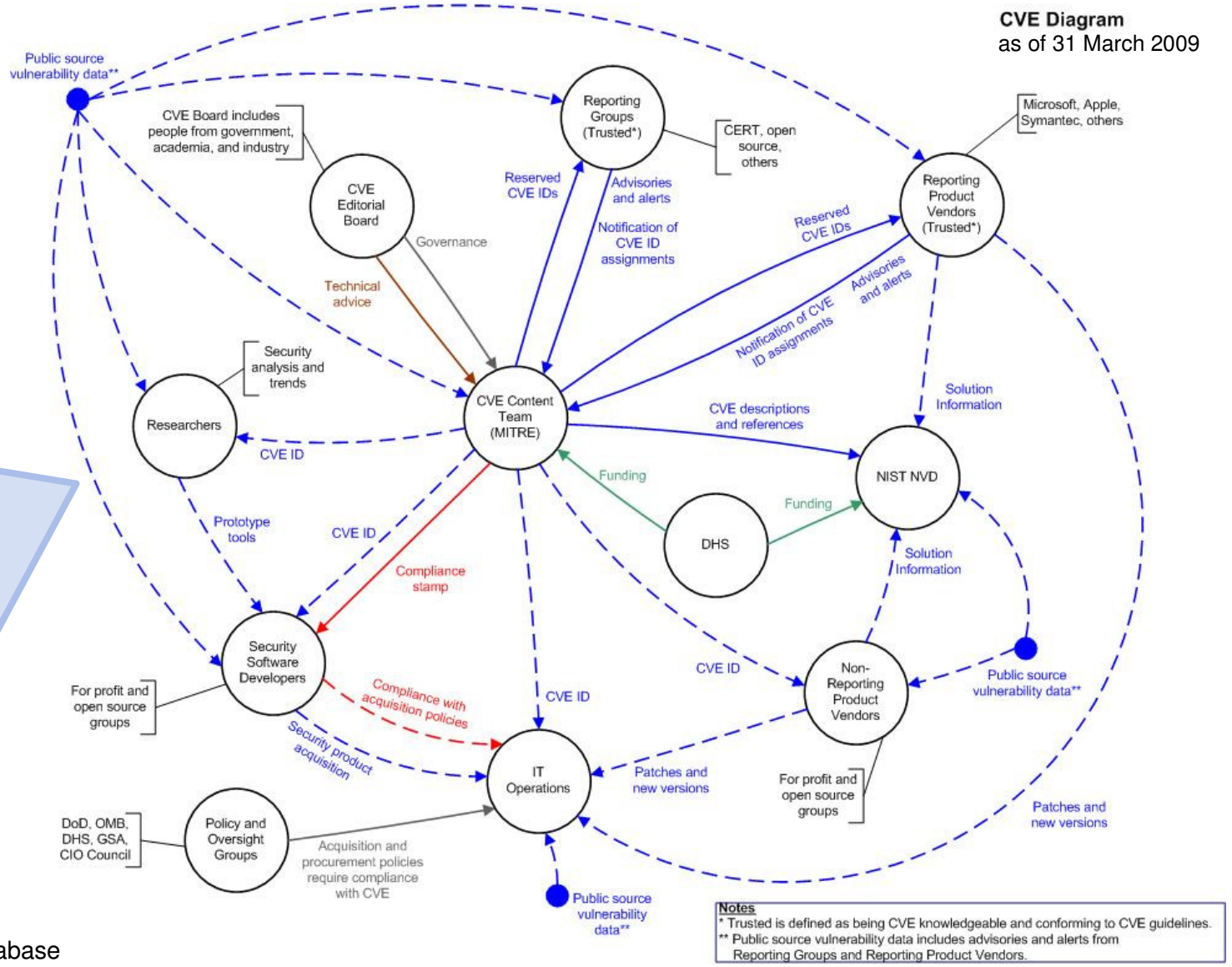
→	Green	Funding
→	Blue	Product
→	Brown	Service
→	Gray	Governance
→	Red	Compliance
→	Orange	Endorsement



CVE: Common Vulnerability Enumeration
CVE is a registered trademark of The MITRE Corporation

Sample CVE Value Map -2

- Independent organizations collaborate with minimal formalities
- We are working with networks or lattices of relationships
- "Distance" between an assurance solution and operational use is often large and complex



NVD: National Vulnerability Database

View: Potential Assurance Results (Q2, 4)

Method: SoS Focus Analysis

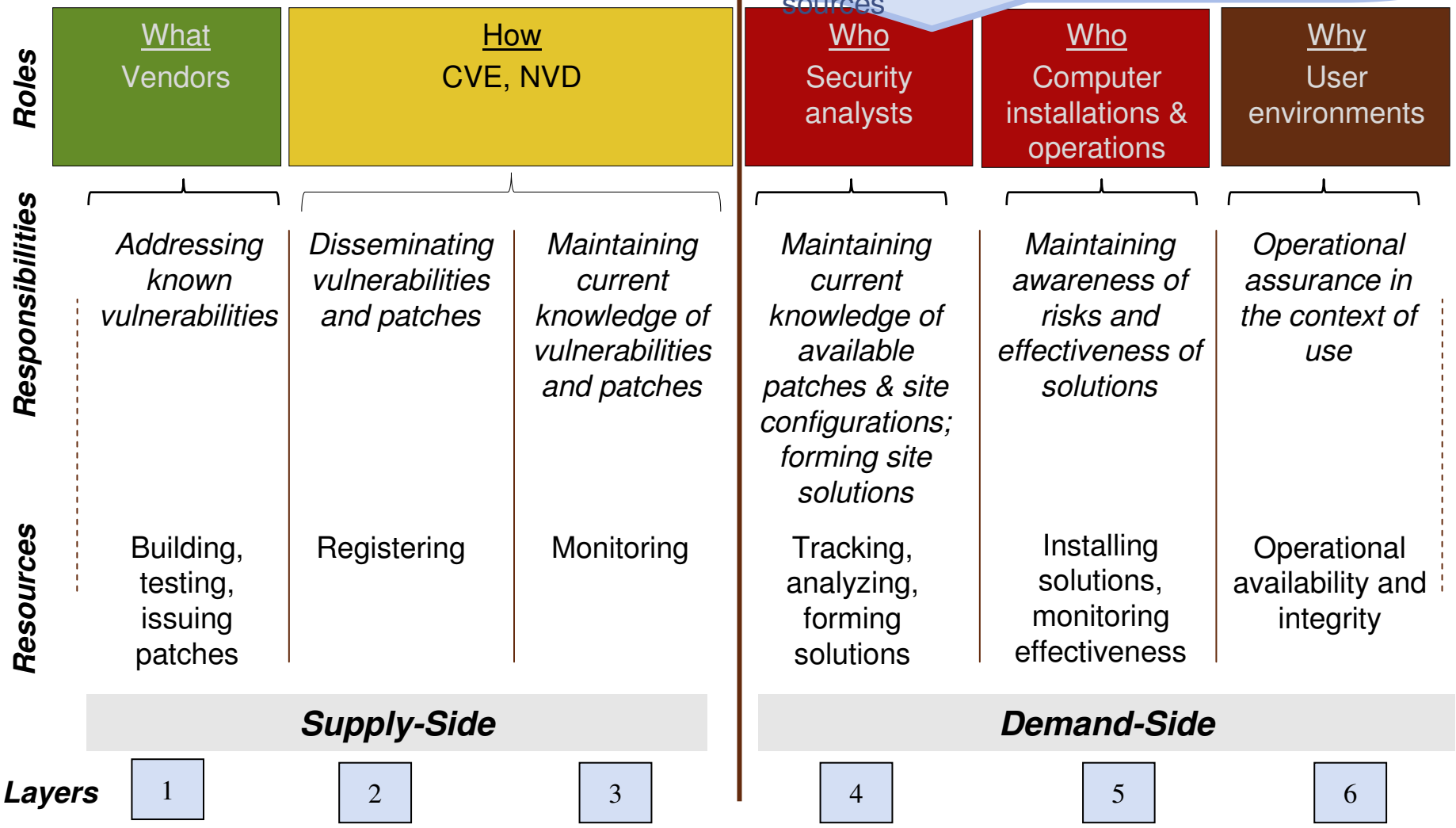
- Produces a resource alignment model needed to bridge between suppliers of assurance solutions and operational users
- Oriented to defining critical collaborations within complex, socio-technical systems (of systems) domains

Selected insights

- Characterizes the layers of organizations and solutions between suppliers and operational users
  - Identifies critical resources to link from assurance solutions to operational results for the selected assurance capability
  - Identifies potential gaps and inefficiencies

SoS Focus Analysis with CVE

- Strong emphasis on supply-side assurance solutions
- Areas of potential inefficiencies: where tacit knowledge is held and 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

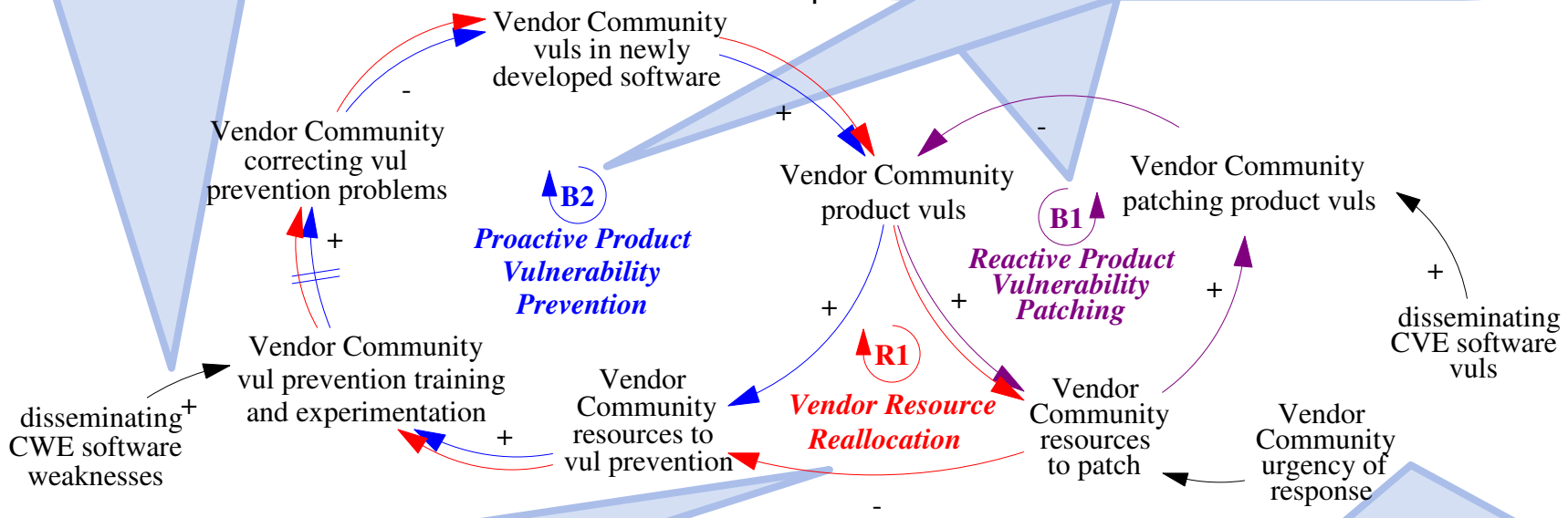
Selected insights

- 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 historically promoted reactive practices
  - CVE-induced market pressures beginning to promote proactive practices
- The models provide a structured way to approach discussions among solution 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 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 for improvement 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 pilot with vulnerability management as a selected assurance capability area
- Finishing a report on the modeling framework and its pilot use

Next Steps

Develop scenarios for usage that could support the DoD community

- Government organizations analyzing the impact of assurance-related policy decisions
- A diagnostic when things don't seem to be working
- Support for funding decisions

Apply the framework to a second assurance capability area

- Selected malicious code prevention and management
- Strengthen understanding of the customer/user (i.e., the demand side)

Contact Information

Lisa Brownsword

Senior Member, Technical Staff

Research, Technology, and System Solutions (RTSS) Program

+1 703-908-8203

llb@sei.cmu.edu

Carol C. Woody, PhD.

Senior Member, Technical Staff

Networked Systems Survivability (NSS) Program

+1 412-268-9137

cwoody@cert.org

Christopher J. Alberts

Senior Member, Technical Staff

Acquisition Support Program (ASP)

+1 412-268-3045

cja@sei.cmu.edu

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.