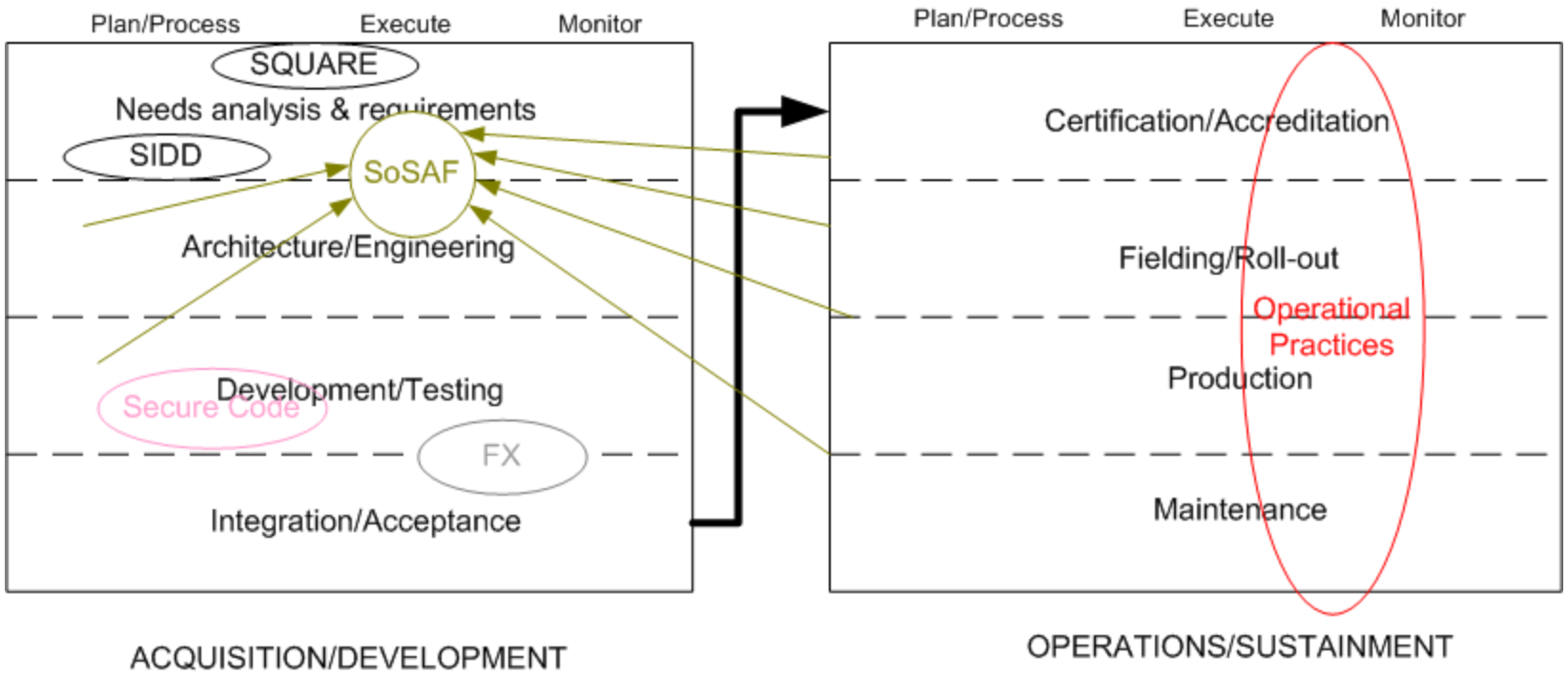
A Toolbox for Improved Security

A Blended Approach

Nancy R. Mead
Software Engineering Institute

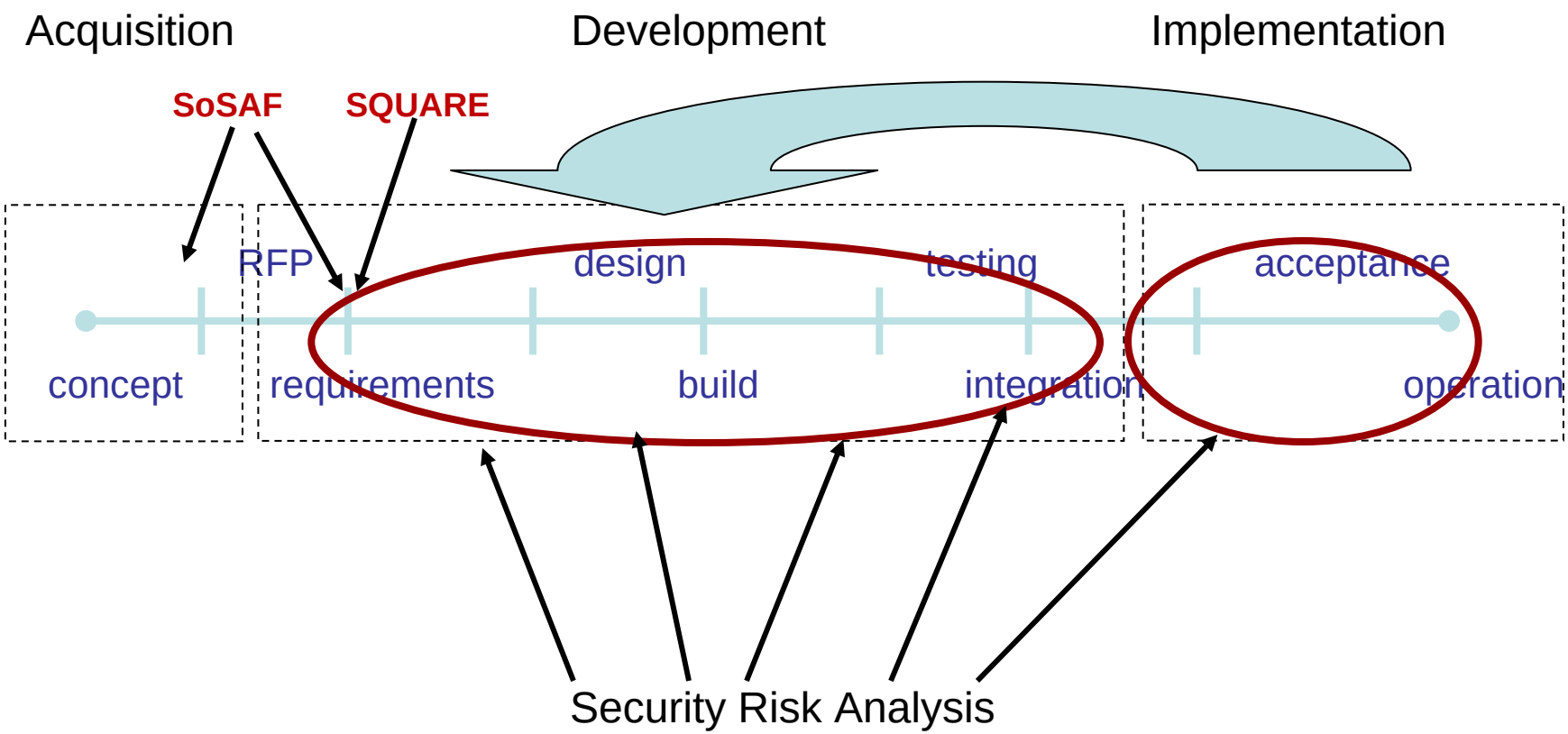
© 2009 Carnegie Mellon University

CERT Research Areas in the SDLC



© 2009 Carnegie Mellon University

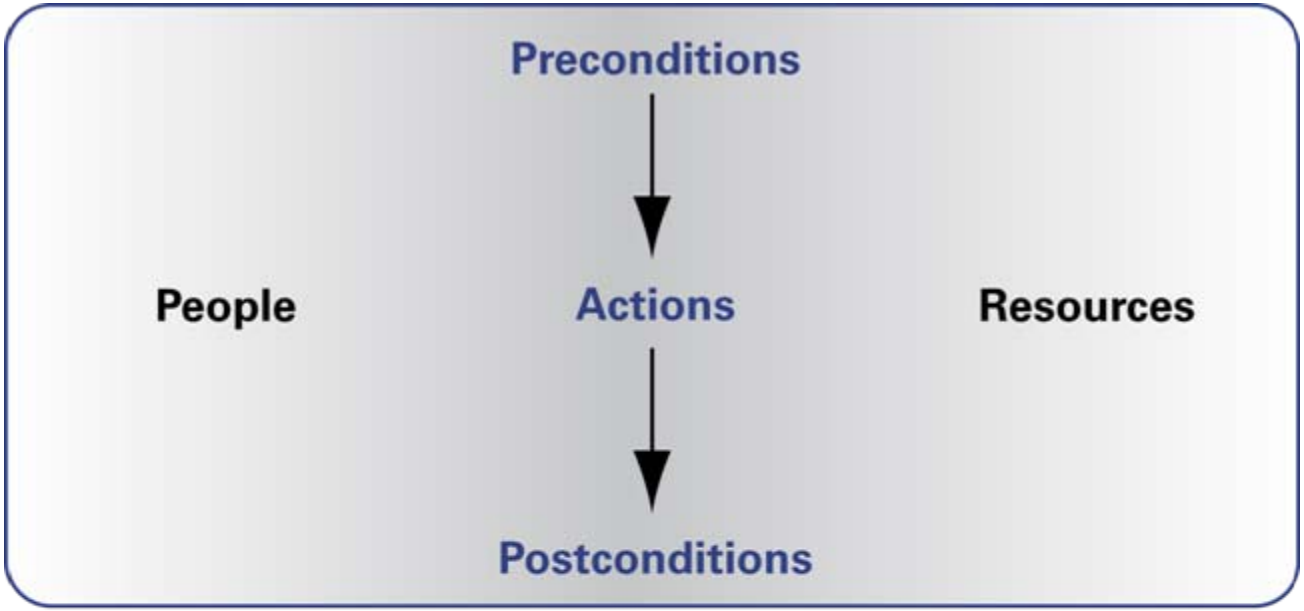
Tools and the SDLC



Security Investment Decision Dashboard

© 2009 Carnegie Mellon University

System of Systems Assurance Framework (SoSAF)



Stresses → **Acceptable Outcomes**

Analysis

- ***Potential failure conditions***
- ***Likelihood of error conditions***
- ***Impact of occurrences***
- ***Recovery strategies***

© 2009 Carnegie Mellon University

Security Quality Requirements Engineering (SQUARE)

Method for identifying software security requirements

Who is involved ?

- stakeholders of the project
- requirement engineers with security expertise

In the SQUARE approach, security requirements are

- treated as add-ons to the system's functional requirements, *but*
- carried out in the early stages
- specified in similar ways as software requirements engineering and practices
- carried out through a process of nine discrete steps

© 2009 Carnegie Mellon University

Security Investment Decision Dashboard (SIDD)

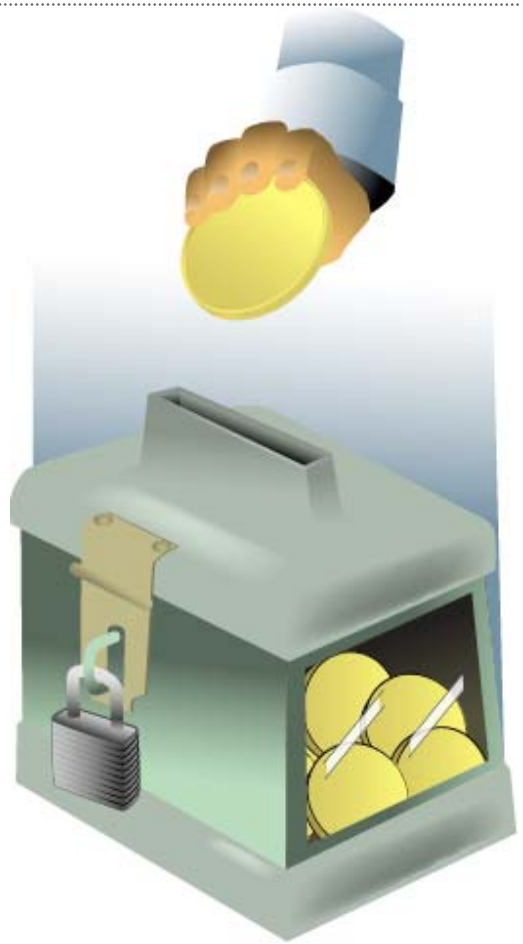
Make security investment decisions in the same fashion as other business investment decisions

Use business-based criteria

Engage leaders in establishing criteria priorities

Track investment priorities, performance, and results over time

Ensure that investments in security directly support business objectives.



© 2009 Carnegie Mellon University

Scenario 1: Program Office Toolbox

Assemble user-focused scenarios and articulate the needs for security based on potential failures (critical interfaces and hazard points) at the program office (SoSAF).

Construct security requirements to inform the acquisition effort for each segment of a system of systems using the scenarios as a guide (SQUARE).

Do investment tradeoff analysis during acquisition, initially and over time (SIDD).

© 2009 Carnegie Mellon University

Scenario 2: Making Tough Choices

Organization can't afford the proposed solution for security

- Selections among security requirements/solutions or even decisions among qualities
- Rationally determine what they can and cannot do – informed by assurance case (SIDD)
- Better redevelop the security requirements for the platforms as part of acquisition effort (SQUARE)

© 2009 Carnegie Mellon University

Scenario 3: Blended Analysis for a Project

Build user scenario and drive through to a proposed assurance case for an acquisition (SoSAF).

Use SoSAF output as SQUARE input to elicit requirements for the acquisition (SQUARE).

Prioritize security requirements; perform investment tradeoff analysis based on the assurance case (SIDD).

© 2009 Carnegie Mellon University

Benefits of the Blended Approach

- Establishes a shared vision for stakeholders and developers of what the system is to do operationally that can be used throughout the remainder of the life cycle.
- Establishes validation criteria for security integration testing (validate the planned operational mission thread)
- Defines tradeoff choices made early in development in such a way that choices can be revisited when the threat environment changes
- Provides a context for defining and verifying quality choices

© 2009 Carnegie Mellon University

Toolbox Elements:

Brief description of each method

© 2009 Carnegie Mellon University

System of System Assurance Framework (SoSAF)

Defining and evaluating successful completion of an integrated mission thread or business process (functions as intended)

Process:

- Identify an integrated mission thread (specific example)
- Identify successful completion criteria for mission thread
- Describe selected critical steps required to complete the thread (end to end) - sequenced activities, participants, and resources
- Identify and analyze ways the selected critical steps may not function as intended and opportunities for mitigation

© 2009 Carnegie Mellon University

An Approach for Quality Analysis

Context and change are critical to quality analysis

- Select the qualities to be evaluated with respect to operational change
- Selected qualities must be clearly defined for the context
- Build one or more detail operational flows incorporating information about the selected qualities

Complexity is unavoidable but analysis cannot consider everything

- Success of the operational flow must be defined
- Focus on the areas most critical to operational success

Failure is assumed to result from a combination of small problems that drive operational execution outside of expected behaviors

- Failure potentials can be characterized as stresses
- Stresses exhibit behaviors that can be identified and monitored
- Mitigation is focused on stress management

© 2009 Carnegie Mellon University

Tolerate Stresses

Inconsistencies (mismatches) must be assumed as we compose systems.

- Systems developed at different times with variances in technology and expected usage
- A system will not be constructed from uniform parts: always some misfits, especially as the system is extended and repaired

Work processes:

- Mission threads are a mix of people, processes, and technology
- Effects of the composition of failures in individual systems on the mission survivability must be considered

Human interactions may be necessary to bridge some mismatches

- Erosion of the people/system boundary – people are an integral part of the system – critical to the completion of a business process
- Mechanisms for people to recognize mismatches must be embedded into the information flows

© 2009 Carnegie Mellon University

SoSAF Analysis Outcomes

Integrated mission thread (business process) example that demonstrates operational execution and captures the effectives of operational dynamics on the planned system and software

Gaps, inconsistencies, and potential failures between design and operation (potential security holes)

Operational changes that may be needed when technology changes

Mitigation opportunities to improve success of the integrated mission thread

© 2009 Carnegie Mellon University

SQUARE for Development – 9 step process

1. Agree on definitions.
2. Identify assets and security goals.
3. Develop artifacts to support security requirements definition.
4. Perform risk assessment.
5. Select elicitation technique(s).
6. Elicit security requirements.
7. Categorize requirements.
8. Prioritize requirements.
9. Inspect requirements.

© 2009 Carnegie Mellon University

SQUARE for Acquisition (A-SQUARE)

Case 1 – Acquisition organization has typical client role for new software.

Case 2 – Acquisition organization does requirements specification (same as original SQUARE).

Case 3 – Acquisition organization is purchasing COTS software.

© 2009 Carnegie Mellon University

A-SQUARE Example Case 1 – New Development

Acquisition steps if security requirements engineering process is unknown

	Step	Input	Techniques	Organizational Responsibility	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Acquisition organization, contractor	Agreed-to definitions
2	**Identify assets and security goals**	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Acquisition organization, contractor	Assets and goals
3	***Contractor identifies security requirements***	*Assets and goals*	*Requirements engineering approach selected by contractor*	*Contractor*	*Initial selected requirements, documentation of decision making process and rationale*
4	**Review of requirements by acquisition organization**	Initial selected requirements	Traditional review	Acquisition organization, contractor	Final requirements

© 2009 Carnegie Mellon University

A-SQUARE Case 3

Process for acquiring COTS software

	Step	Input	Techniques	Participants	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Acquisition organization – stakeholders, security specialists	Agreed-to definitions
2	**Identify assets and security goals**	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Acquisition organization – stakeholders, security specialists	Assets and goals
3	**Identify preliminary security requirements**	Assets and goals	Work session	Acquisition organization – security specialists	Preliminary security requirements
4	**Review COTS software package information and specifications**	Assets, goals, preliminary security requirements	Study security features of various packages and documents them, in a spreadsheet, for example	Acquisition organization – security specialists, COTS vendors	Spreadsheet of security features of various packages

© 2009 Carnegie Mellon University

A-SQUARE Case 3

Process for acquiring COTS software

	Step	Input	Techniques	Participants	Output
5	**Finalize security requirements**	Preliminary security requirements, features of various packages	Work session – use the spreadsheet to refine and modify the preliminary security requirements to arrive at a final set	Acquisition organization – security specialists	Final security requirements
6	**Perform tradeoff analysis**	Final security requirements, spreadsheet of security features	Tradeoff analysis of COTS products relative to final security requirements	Acquisition organization – stakeholders, security specialists	Prioritized list of COTS products relative to security requirements
7	**Final product selection**	Prioritized list of COTS products relative to security, other important COTS product features	Tradeoff analysis	Acquisition organization – stakeholders	Final COTS product selection

© 2009 Carnegie Mellon University

SIDD Decision Categories - 1

Cost: Estimated total cost to accomplish the investment

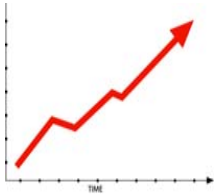
Criticality & Risk: Degree to which the investment contributes to meeting business objectives and risk management goals

Time & Effort Required: Level of staff hours and time to break even

© 2009 Carnegie Mellon University

SIDD Decision Categories - 2

Feasibility: Likelihood of investment success



Positive Interdependencies: Reasonable changes to existing processes? Paves the way for future work?

Involvement: Level of required involvement and buy-in

Measurability: How measurable the investment outcome is

© 2009 Carnegie Mellon University

Using SIDD

Senior leadership ranks investment decision category criteria (7)

Cross-organizational steering council ranks indicators (3-6 per category)

- Cross check with senior leadership

Candidate investments scored against criteria and indicators using a 5-point scale

Investment scores calculated, compared, and discussed; tracked over time

© 2009 Carnegie Mellon University

SIDD: Example Scoring

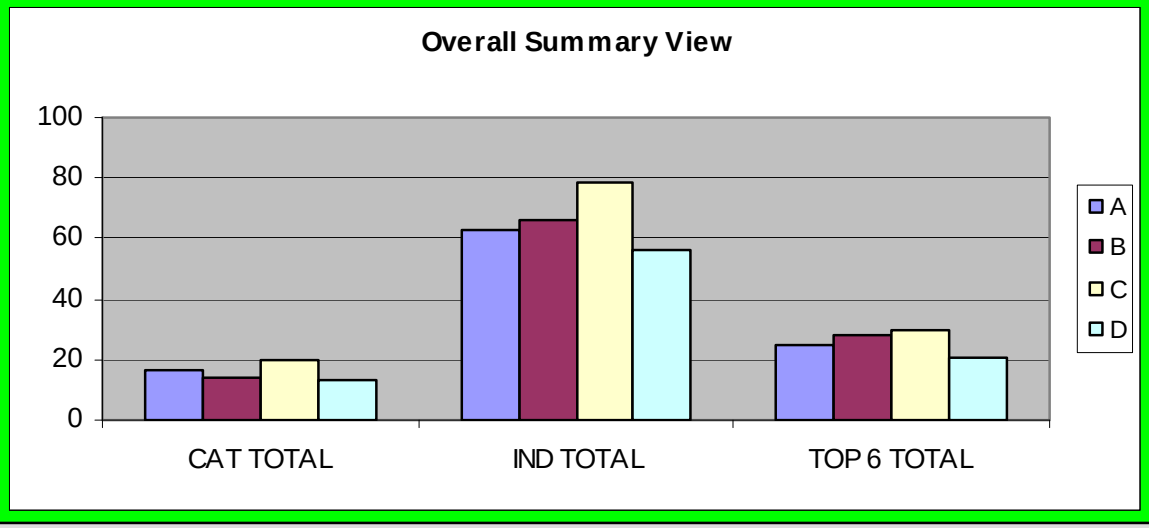
				1	2	3	4	5		
	Category / Indicator	**Cat Rank (1-7)**	**Rank (1-33)**	don't do	unlikely	later?	soon	do	**MULT**	**SCORE**
Cat	**Cost**	2		v high	high	med	4	v low	4	**4**
Consider	Estimated total cost to accomplish this investment, taking into account the potential cost savings and/or risk reduction to the organization									
Indicators	Overt cost in dollars at outset to accomplish this investment		6	v high	high	3	low	v low	3	**3**
	Estimated life-cycle cost in dollars over time to sustain this investment		7	v high	high	med	low	5	5	**3.75**
	Cost of NOT doing this investment, in terms of potential exposure and residual risk (high = investment is more necessary)		1	v low	low	med	4	v high	4	**4**
	Potential cost savings to organization beyond breakeven point, if quantifiable (ROI), over time (high = better)		9	v low	low	med	4	v high	4	**3**

© 2009 Carnegie Mellon University

DASHBOARD SAMPLE

	Candidate Investments											
	A	B	C	D	etc.							
CAT TOTAL	16.25	14.25	19.75	13.5								
IND TOTAL	62.5	66.25	78.75	56.5								
TOP 6 TOTAL	24.75	28	30	21								

Project	Description
A	Integrate architectural risk analysis into the standard SDLC.
B	Integrate secure coding practices for C and C++ into the standard SDLC.
C	Integrate the use of static code analysis tools into the standard SDLC.
D	Integrate security requirements engineering using SQUARE into the SDLC.



© 2009 Carnegie Mellon University

Future Directions:

Where do we go from here?

© 2009 Carnegie Mellon University

Plans for Blended Approach

Pilot projects

Educational materials

Tools

© 2009 Carnegie Mellon University

Pilot Projects of Interest

Systems of systems projects in the early part of the acquisition or development life cycle

Projects with a critical concern for improved security

© 2009 Carnegie Mellon University

Questions?

© 2009 Carnegie Mellon University

References

Ellison, R., Goodenough, J., Weinstock, C., and Woody, C. *Survivability Assurance for Systems of Systems,* Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2008-TR-008, http://www.sei.cmu.edu/publications/documents/08.reports/08tr008.html

Alberts, C., Smith II, J., and Woody, C. *Multi-view Decision Making (MVDM) Workshop*, Software Engineering Institute, Carnegie Mellon University , CMU/SEI-2008-SR-035, http://www.sei.cmu.edu/publications/documents/08.reports/08sr035.html

Mead, N.R., Hough, E., Stehney, T. *Security Quality Requirements Engineering (SQUARE) Methodology*, Software Engineering Institute, Carnegie Mellon University , CMU/SEI-2005-TR-009, www.sei.cmu.edu/pub/documents/05.reports/pdf/05tr009.pdf

Mead, N.R., "SQUARE Process" Carnegie Mellon University, September 17, 2008 https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/requirements/232-BSI.html

Allen, Julia. "Making Business-Based Security Investment Decisions – A Dashbaord Approach." Carnegie Mellon University, September 23, 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/985-BSI.html

© 2009 Carnegie Mellon University