New Directions in Risk Management at the SEI

Ray C. Williams
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 2003 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

The Software Engineering Institute

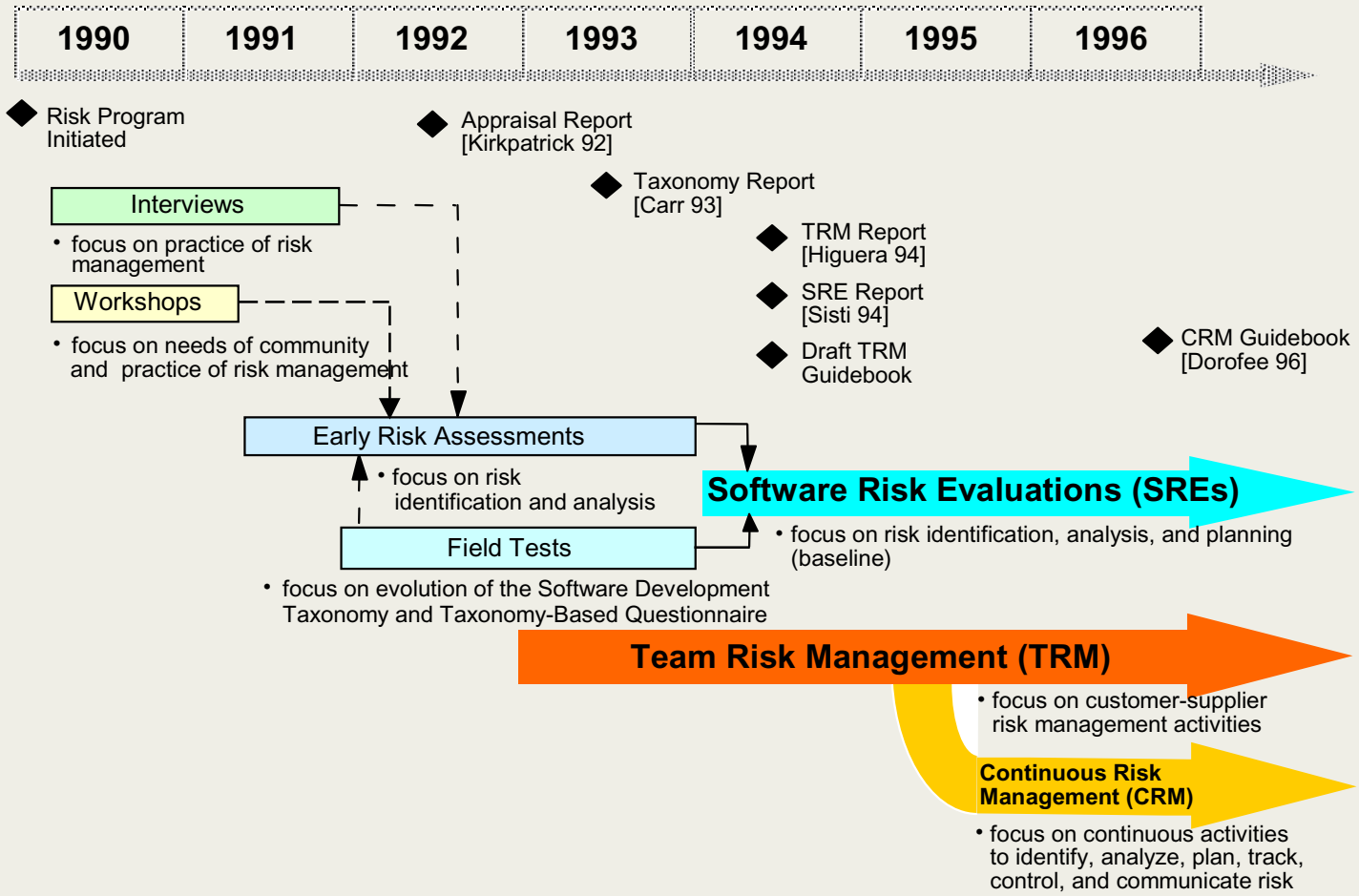
- *A unit of Carnegie Mellon University, Pittsburgh, PA*
  - A Federally-Funded Research and Development Center (FFRDC)
  - Established 1984
  - Predominantly supports the DoD, but also civil agencies of the Federal Government (e.g., NASA, IRS, FAA) and a few corporate entities
  - FFRDC business model similar to MIT's Lincoln Labs, mostly funded by clients on as-needed basis

- *Primarily focused on improving the development and acquisition of software-intensive systems*
  - Process improvement (SW-CMM®, CMMI®, PSP®, risk management)
  - Diagnostics (architecture, COTS, software risk evaluation, network assets)

®CMM, CMMI, and PSP are registered trademarks of Carnegie Mellon University

© 2003 by Carnegie Mellon University

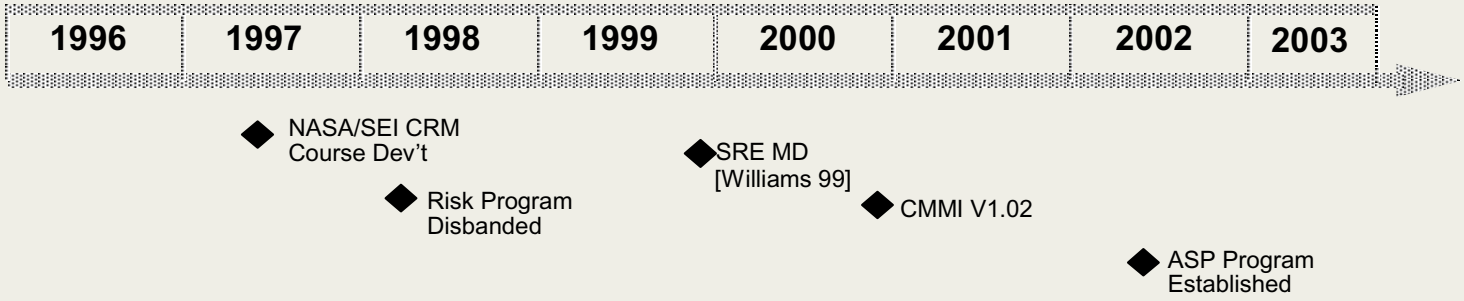
History of SEI Risk Management[1]

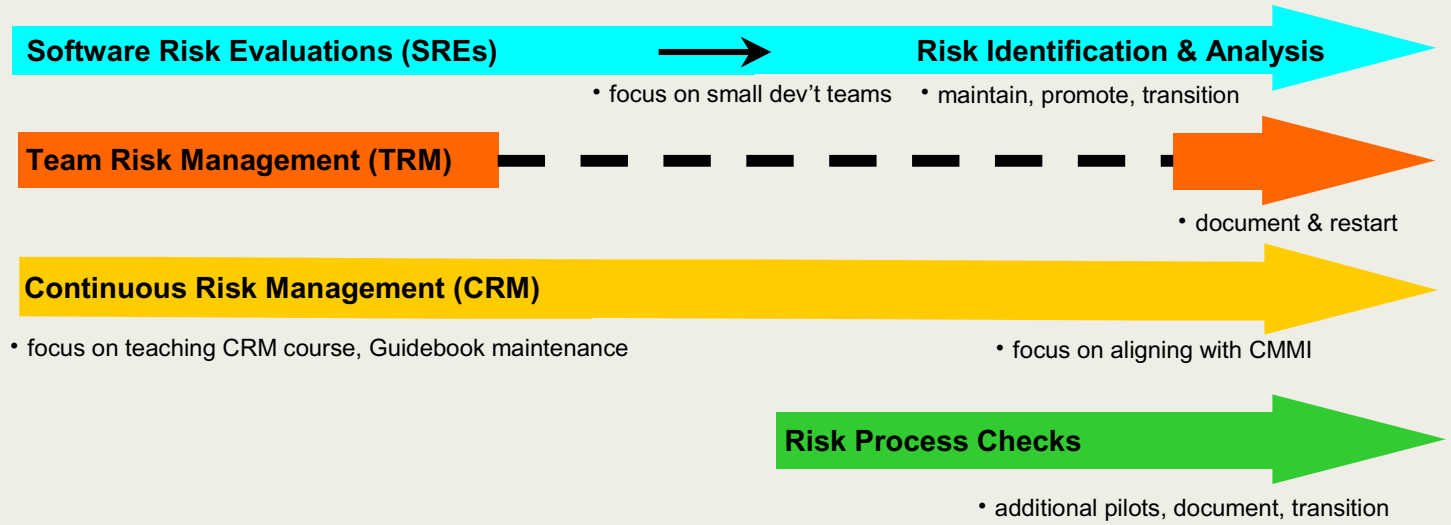


© 2003 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

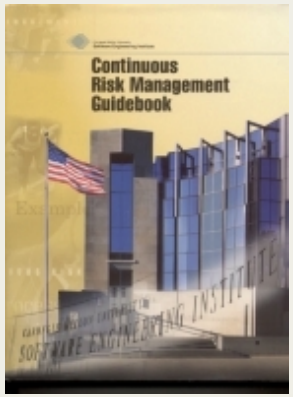
History of SEI Risk Management$_2$





© 2003 by Carnegie Mellon University

New Directions in Continuous Risk Management (CRM)

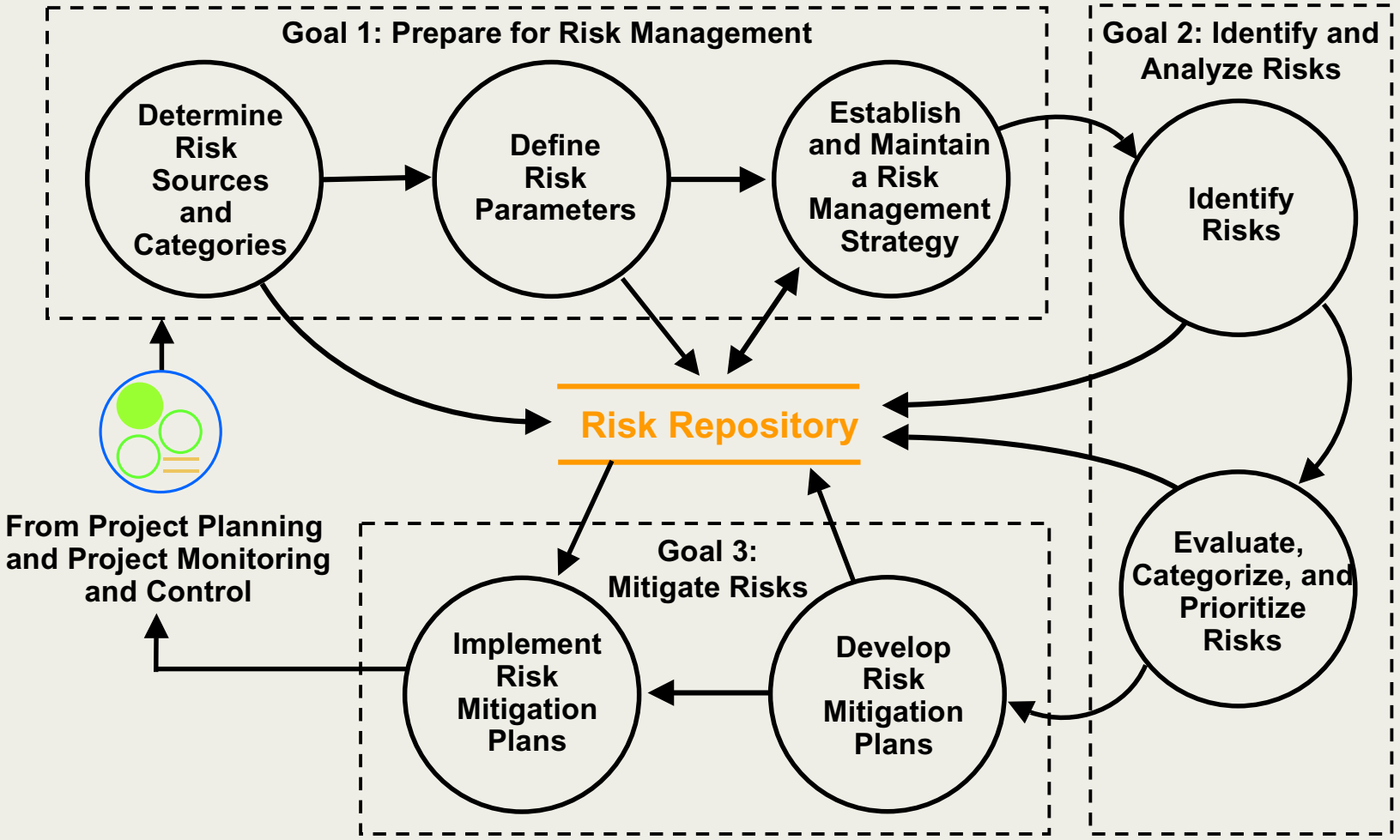


- Aligning with the Capability Maturity Model Integration (CMMI) process area on Risk Management
- Moving away from the idea that the objects in risk management databases (risk repositories) are “risks”
- Maximizing the number of objects that are fed into risk repositories
- Building the capability of the risk management process to handle a ten-fold (or more) increase in input through classification into “risk areas”

© 2003 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Risk Management Process Area (CMMI)

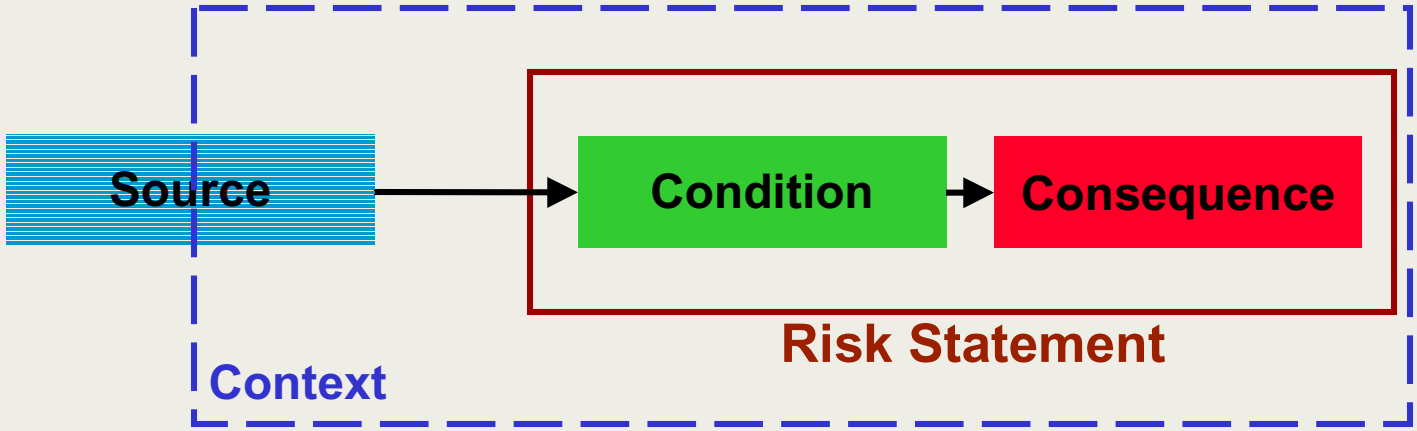


© 2003 by Carnegie Mellon University

The Risk Statement

A “standard” format for risk statements provides:

- clarity
- consistency
- a basis for future risk processing



A good Risk Statement is

- fact-based
- actionable
- brief

© 2003 by Carnegie Mellon University

New Directions in Risk Identification and Analysis (RI&A)

- Incorporating other RI&A methods, e.g.
  - Architectural Tradeoff Analysis Method (ATAM)
  - COTS Usage Risk Evaluation (CURE)
  - Software Quality Attribute Exercise (SQAE – developed by MITRE)
  - Independent Technical Evaluations (ITAs)
- Following a medical diagnostic analogy
  - Providing tools to let SEI Chief Engineers function like Personal Care Physicians (PCPs)
  - Creating a “roadmap” for risk identification that provides at least 3 entry points:
    - The “Thermometer” (self diagnosis)
    - The “Routine Physical”
    - The “Emergency Room”

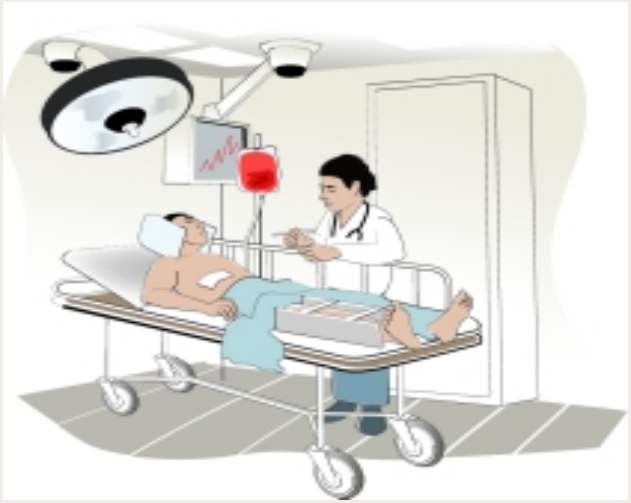
© 2003 by Carnegie Mellon University

The Healthcare Analogy

Three types of diagnostic approaches

Routine physical

Self diagnosis



Emergency room/triage

© 2003 by Carnegie Mellon University

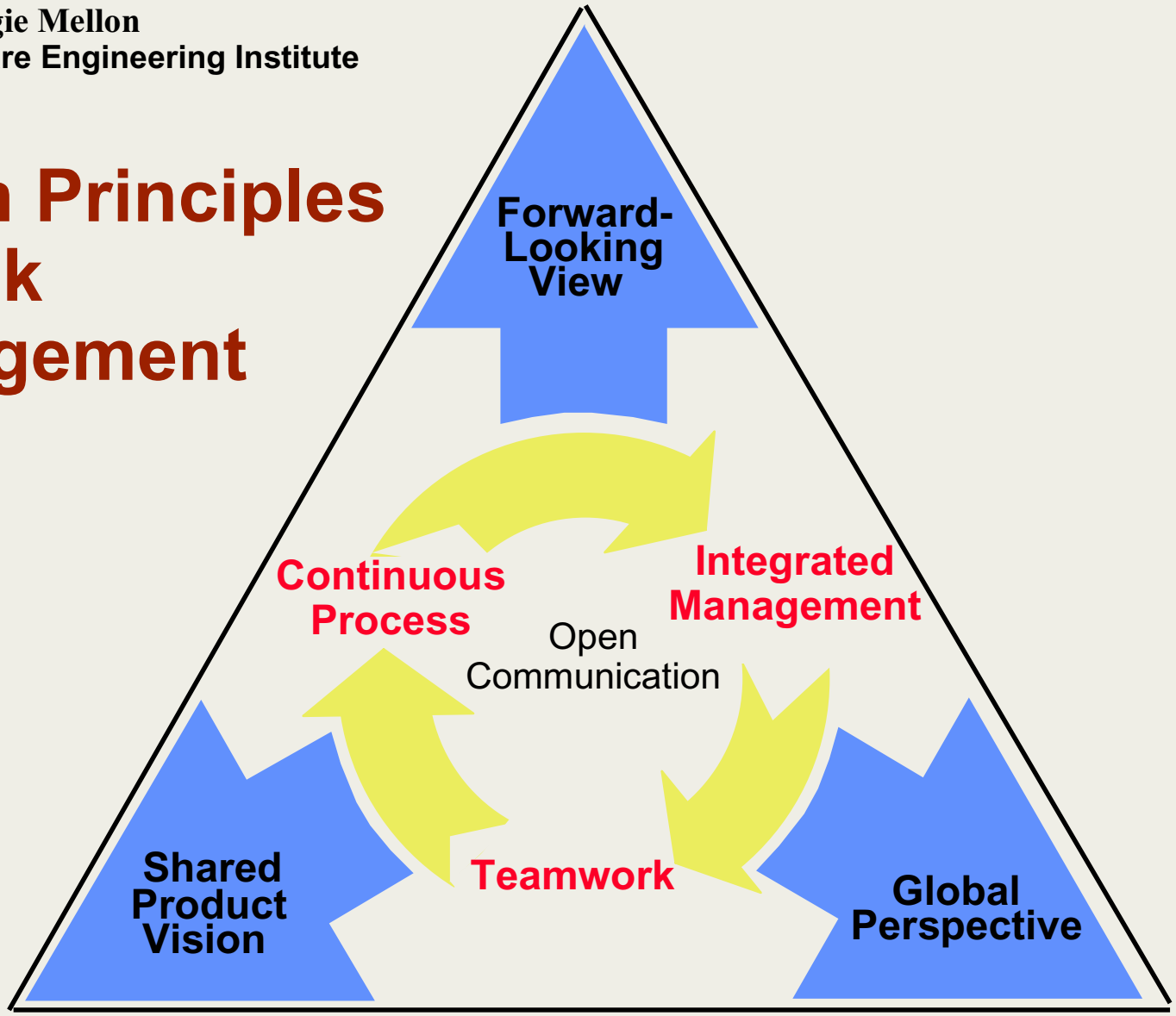
Rejuvenating Team ("Joint")* Risk Management$_1$

- Team Risk Management (TRM) is the discipline of Identifying, Analyzing, Planning, Tracking, and Controlling risks is a larger government program context.
- It focuses on breaking down the risk communications barriers between
  - A government program office and its prime contractor(s)
  - The primes and their subcontractors
  - Multiple co-equal programs that are linked together for overall government acquisition or strategic success

* We're considering changing the name from "Team" to "Joint" because of confusion with other initiatives, e.g. Team Software Process, Integrated Product and Process Development teams.

© 2003 by Carnegie Mellon University

Seven Principles of Risk Management



© 2003 by Carnegie Mellon University

Rejuvenating Team Risk Management$_2$

- The SEI's (and NASA's) Continuous Risk Management approach is focused on the development team, which is expected to have clear understanding of *Shared Product Vision*, *Global Perspective*, and *Forward-Looking View.*
- TRM was designed to address the cases when these perspectives are not shared between organizations.
- There were signal successes in TRM up to 1998—in the Navy E6 program, Navy CPMU program, and in the NRO IMINT Directorate—but since then the effort has languished from lack of collaborative opportunities.
- The key documentation for the TRM discipline has never been published (the original concept was for a *Team Risk Management Guidebook* to be a bookshelf companion to the *Continuous Risk Management Guidebook*).

© 2003 by Carnegie Mellon University

New Concept: The *Risk Process Check*

- Application: A large, multilevel DoD program
- We were asked, “How well does our risk management process work?”
- Created a “model-less” evaluation approach
  - Creation of initial, explicit “mental model” of how we are told the risk management process operates
  - Site visits, interviews, survey instruments
  - Application of the “Green Engineer” test
  - Revision of the “mental model” to reflect how the risk process *really* operates
- Later applied in two NRO contractor locations
- Currently inactive for lack of sponsorship and collaborations

© 2003 by Carnegie Mellon University

The "Green Engineer" Test

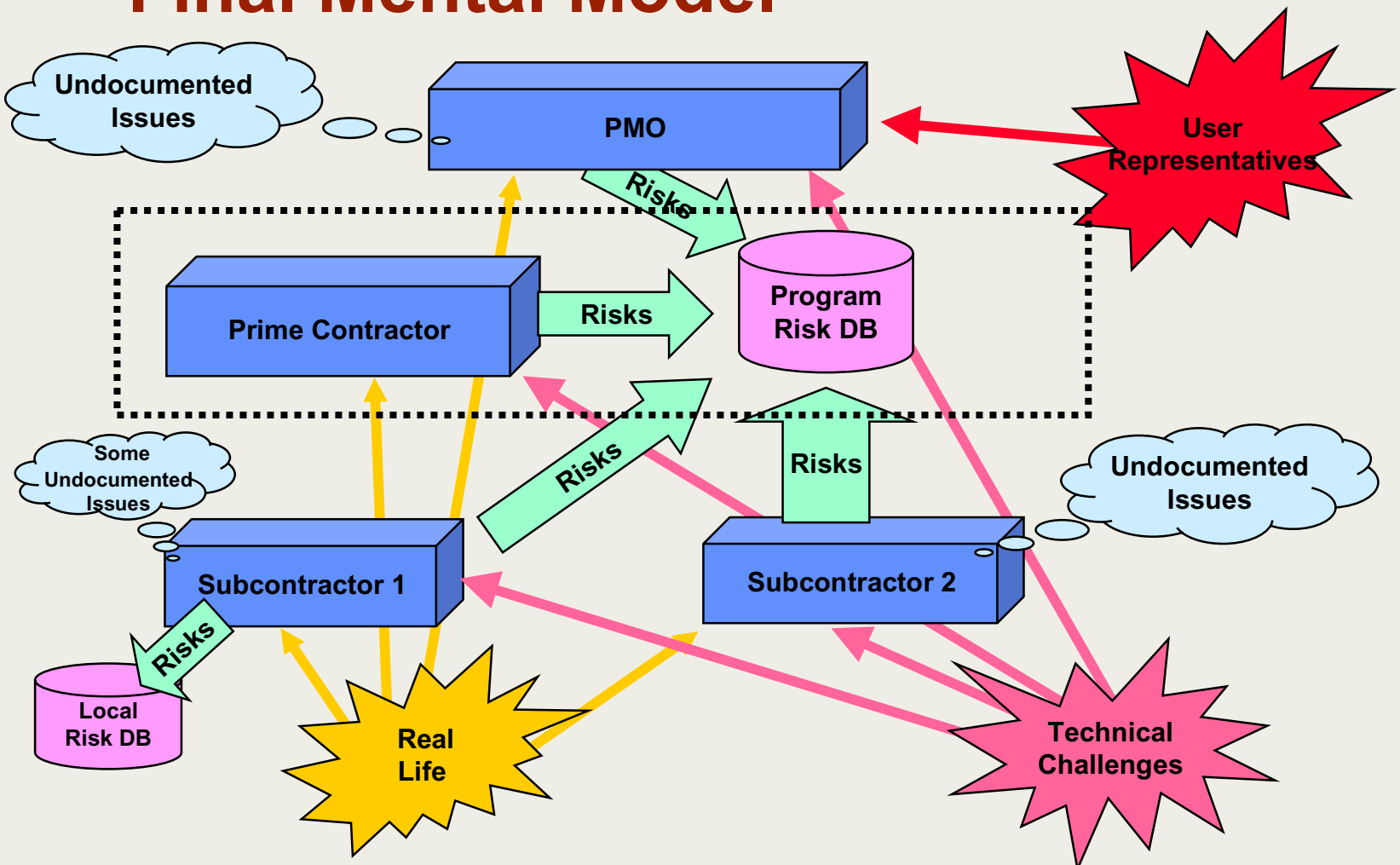
Assume a "green" engineer in any of the program's organizations (someone at the bottom of the program's decision-making hierarchy) stumbles onto a "show-stopper" risk in the current technical approach.

How **quickly** and how **accurately** will the following happen?

- The risk is *recognized*
- The risk is *recorded* in the risk management system
- The risk makes it to the *appropriate decision-making level* in the program
- An appropriate risk mitigation strategy is determined and *jointly* agreed upon

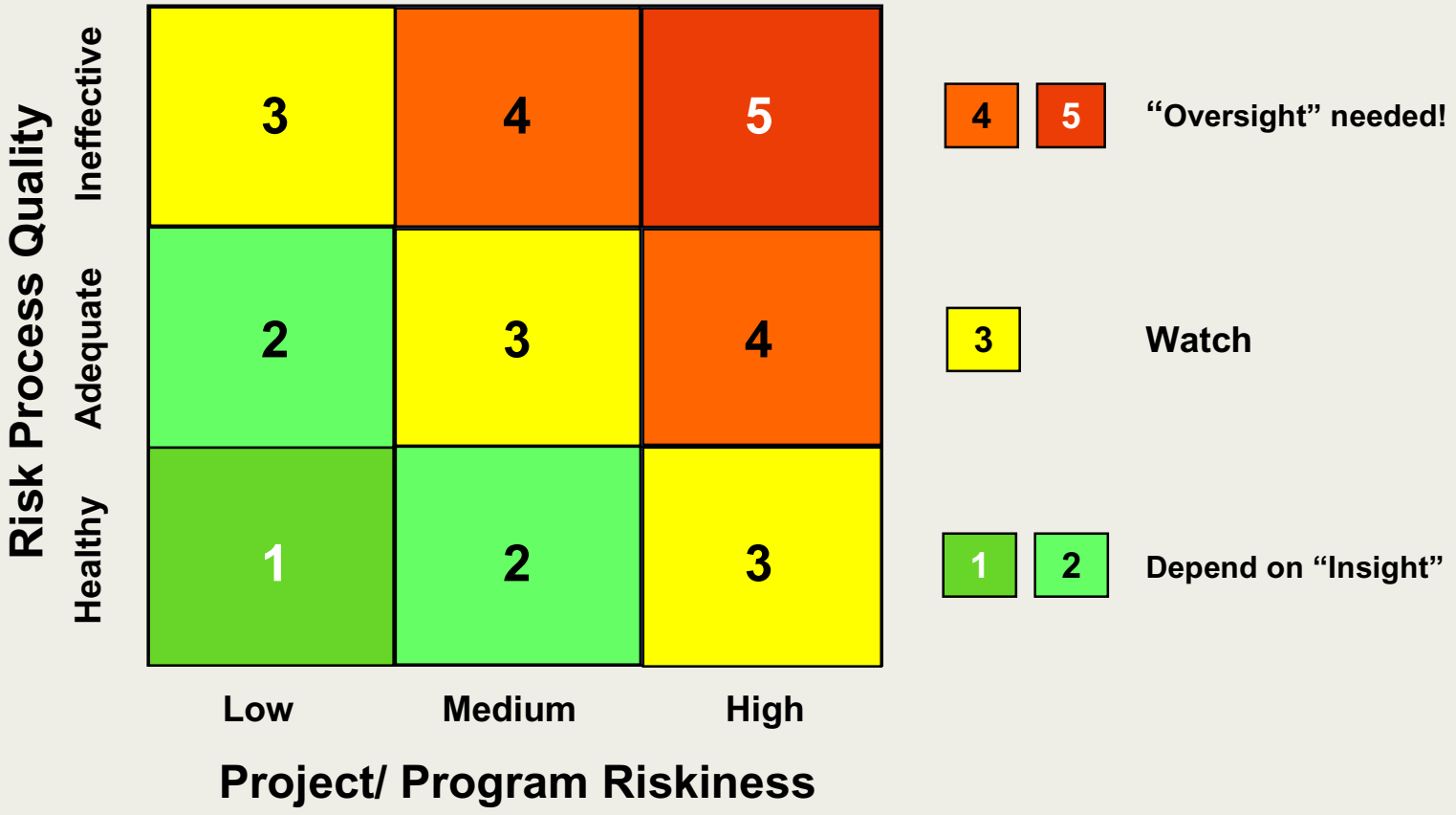
© 2003 by Carnegie Mellon University

Final Mental Model



© 2003 by Carnegie Mellon University

"Insight" or "Oversight"?



© 2003 by Carnegie Mellon University

Summary

- SEI risk management work was curtailed in 1998, but has continued at more modest level and in other forms
- Under the Acquisition Support Program, we are beginning to revitalize SEI risk management work focusing on *Risk Identification & Analysis* and *Team* ("Joint") *Risk Management*
- *Continuous Risk Management* is mostly in maintenance mode, with some new directions emerging in the SEI's version of the CRM course
- *Risk Process Checks* show real promise as a new tool to help programs assess and improve the effectiveness of their risk management, but this initiative is currently shelved for lack of sponsorship and piloting opportunities

© 2003 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Contact Information

Telephone	412 / 268-5800
FAX	412 / 268-5758
Internet	customer-relations@sei.cmu.edu
World Wide Web	http://www.sei.cmu.edu
U.S. mail	Customer Relations Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890

© 2003 by Carnegie Mellon University