The CMMI RSKM Process Area as a Risk Management Standard

Ray C. Williams
Carnegie Mellon University
Software Engineering Institute

July 12, 2006
All Risk Management Standards Share a Common Fault

They all take the position, “I am smarter about risk management than you are. Do as I say and you will begin practicing effective risk management.”

- No proof is provided
- They claim broad support of their community, but are written by a select group of self-identified “experts”
- No one appears to be doing any research to prove that the specified standards actually lead to effective risk management
- There is no operational definition of “effective risk management” anyway
Most Risk Management Standards Fail Their Audience in Other Ways

- They have no training support
- They have no mechanisms for measuring compliance
- They avoid issues on which the “experts” disagree
- They conflict with one another on common terminology
The CMMI RSKM Process Area Shares Some of These Failings

- At Capability Levels (CLs) 1 – 3, RSKM is purely a compliance model and effectiveness is asserted, not proven
- It uses its own terminology
- It doesn’t show you an example of a written “risk” – too controversial

But...

- It is supported by training
- It has a defined appraisal process with considerable experiential data already gathered
- At CLs 4 & 5, it provides an avenue for measuring, proving, and improving effectiveness

*(however, very few have been appraised at CL4 or 5 in RSKM...)*
CMMI RSKM Requires the Basics...

Goal 1: Prepare for Risk Management
- Determine Risk Sources and Categories
- Define Risk Parameters
- Establish and Maintain a Risk Management Strategy
- Implement Risk Mitigation Plans

Goal 2: Identify and Analyze Risks
- Identify Risks
- Evaluate, Classify, and Prioritize Risks

Goal 3: Mitigate Risks
- Develop Risk Mitigation Plans

Risk Repository

From Project Planning and Project Monitoring and Control
CMMI RSKM is a 6-Level Risk Management Maturity Model

**Level 0: Incomplete**
Process is either not performed or is partially performed

**Level 1: Performed**
- Identify work scope
- Perform base practices

**Level 2: Managed**
- Establish an organizational policy
- Plan the process
- Provide resources
- Assign responsibility
- Train people
- Manage configurations
- Identify and involve relevant stakeholders
- Monitor and control the process
- Objectively evaluate adherence
- Review status with higher-level management
CMMI RSKM is a 6-Level Risk Management Maturity Model

**Level 3: Defined**
- Establish a defined process
- Collect improvement information

**Level 4: Quantitatively Managed**
- Establish quality objectives
- Stabilize subprocess performance

**Level 5: Optimizing**
- Ensure continuous process improvement
- Correct common cause of problems
Who Polices Gaps, Conflicts, and Overlaps between CMMI RSKM and Other Risk Management Standards?

To my knowledge, no one...

...and no one should.
What Should INCOSE Do?

Should *not*...
- Police gaps, conflicts and overlaps
- Create its own risk management standard

Should...
- Pick an existing risk management standard to support
- Become an *influencer* of that standard