The CMMI RSKM Process Area as a Risk Management Standard

Ray C. Williams
Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15208
rcw@sei.cmu.edu

Sixteenth Annual International Symposium of the
International Council On Systems Engineering (INCOSE)
8 - 14 July 2006

Abstract. In this position paper, the author asserts that all existing risk management standards promulgate *compliance* with the opinions held by a small sub-community of risk practitioners, rather promoting processes and practices that have demonstrated their *effectiveness* in managing risks in real organizations. The author takes the position that the CMMI RSKM process area, if viewed as a standard, shares this weakness in its basic features; however, when an organization can rise to the higher capability levels in RSKM (Capability Levels 4 and 5), the CMMI holds the promise of promoting and proving effective risk management. To date, however, this promise has not been realized.

.

The Problem with Risk Management Standards

All risk management standards share a common fault: Regardless of the organization that creates and promotes them, they claim broad support from their community and purport to reflect "best practices" in risk management, and yet in each case they have been created by a select group of self-identified "experts" in the field from within the organization. While they may have received pre-publication review by members of a broader community of other "experts" and interested parties, they remain opinion pieces from a small in-group of practitioners who presume to speak for the larger community. 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."

Unfortunately, this assertion has never been put to the test. We in the community of "risk management experts and consultants" have not gathered or analyzed data to prove that what we tell people to do will actually help them manage risks better than if they had simply made up their own processes and approaches.

I will go further: Because of our collegial approach to writing risk management standards, we tend to articulate the areas of risk management practice where we agree with one another (the need to identify risks, analyze them in some way, put together mitigation plans for them, and carry out those plans) while avoiding the points on which we disagree (e.g., how to compose a statement of risk, or the proper approach to doing risk analysis), leaving the user of our standards in the dark about the specifics of *how* to do what our standards "require." And because we each apply our own lexicon within our standards (you say "consequence," I say "impact"; you say "probability," I say "likelihood"…), we leave our community of risk management practice to decide individually which of us they will follow, since that is the only way they can use a consistent lexicon and approach in their own organizations.

If we do not require organizations to be appraised in some way on the degree to which they follow whatever standard they choose for risk management, they can simply assert that they are following a standard ("We follow the PMI PMBoK in our work" or "We follow IEEE Std 1540"). Who's going contradict them? If we *do* require organizations to be appraised against our standard or model, as done for example in the Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠), the organization's focus can become compliance with the letter of the model rather than the selection of processes and approaches that will best assure effective risk management in their own environment.

To a certain degree, the Risk Management (RSKM) process area of Capability Maturity Model Integration (CMMI®) shares these weaknesses. In its basic practices RSKM is no better—and no worse—than the other standards. However, in the practices of its advanced levels (practices which it shares with all the other 24 process areas of the "full up" CMMI model), the RSKM process area provides an avenue for establishing truly "effective" risk management processes and practices rather than merely "compliant" ones, and for the organization to teach us all why they are "effective."

Let's take a look at what makes CMMI RSKM different.

Brief Overview/Review of CMMI RSKM

Basic goals and practices. The three *required* specific goals and seven *expected* specific practices of RSKM are shown graphically in Figure 1. Stated in full, the goals and practices are:

Specific Goal 1: *Preparation for risk management is conducted*

Specific Practice 1.1: *Determine risk sources and categories.*

Specific Practice 1.2: *Define the parameters used to analyze and categorize risks, and the parameters used to control the risk management effort.*

Specific Practice 1.3: *Establish and maintain the strategy to be used for risk management.*

Specific Goal 2: *Risks are identified and analyzed to determine their relative importance.*

Specific Practice 2.1: *Identify and document the risks.*

Specific Practice 2.2: *Evaluate and categorize each identified risk using the defined risk categories and parameters, and determine its relative priority.*

Specific Goal 3: *Risks are handled and mitigated, where appropriate, to reduce adverse impacts on achieving objectives.*

Specific Practice 3.1: *Develop a risk mitigation plan for the most important risks to the project, as defined by the risk management strategy.*

Specific Practice 3.2: *Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate.*

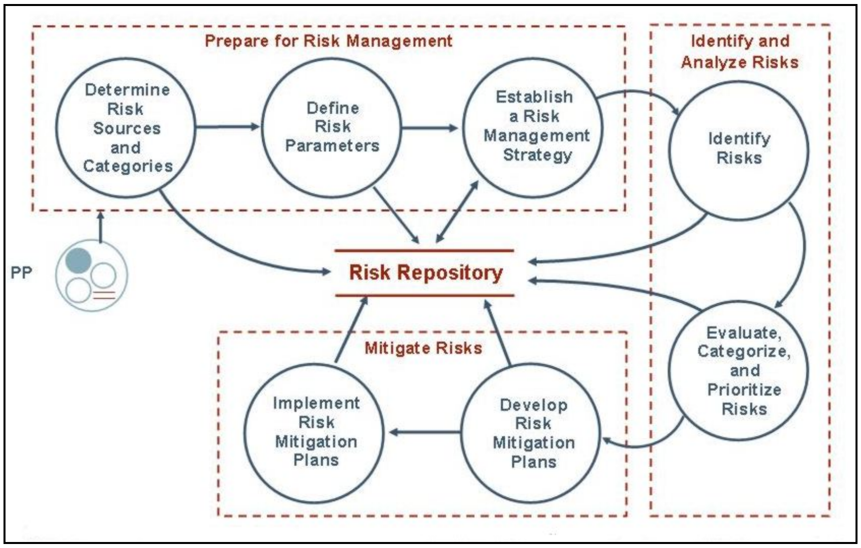
Prepare for Risk Management
Identify and Analyze Risks
Determine Risk Sources and Categories
Define Risk Parameters
Establish a Risk Management Strategy
Identify Risks
PP
Risk Repository
Evaluate, Categorize, and Prioritize Risks
Mitigate Risks
Implement Risk Mitigation Plans
Develop Risk Mitigation Plans

Figure 1—The Risk Management (RSKM) Process Area of CMMI

Capability Levels. In the continuous representation of CMMI, there are six Capability Levels for RSKM (and any of the CMMI process areas, for that matter):

Capability Level 0—Incomplete. RSKM is either not performed or partially performed. One or more of the specific goals of RSKM are not satisfied.

Capability Level 1—Performed. The organization's risk management practices satisfy all of the specific goals of the RSKM process area.

Capability Level 2—Managed. At this level, RSKM is performed, but it is also planned and executed in accordance with policy, employs skilled people having adequate resources to produce controlled outputs, involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description.

Capability Level 3—Defined. At this level, RSKM is "managed" as at capability level 2, but it also follows a process that is tailored from the organization's set of standard processes according to the organization’s tailoring guidelines, and contributes work products, measures, and other process-improvement information to the organizational process assets.

Capability Level 4—Quantitatively Managed. At this level, RSKM is a defined (capability level 3) process that is controlled using statistical and other quantitative techniques. Quantitative objectives for quality and process performance are established and used as criteria in managing the process. The quality and process performance are understood in statistical terms and are managed throughout the life of the process.

Capability Level 5—Optimizing. At this level, RSKM is a quantitatively managed (capability level 4) process that is changed and adapted to meet relevant current and projected business objectives. An optimizing process focuses on continually improving the process performance through both incremental and innovative technological improvements. Process improvements that would address root causes of process variation and measurably improve the organization’s processes are identified, evaluated, and deployed as appropriate. These improvements are selected based on a quantitative understanding of their expected contribution to achieving the organization’s process-improvement objectives versus the cost and impact to the organization. The process performance of the organization's processes is continually improved.

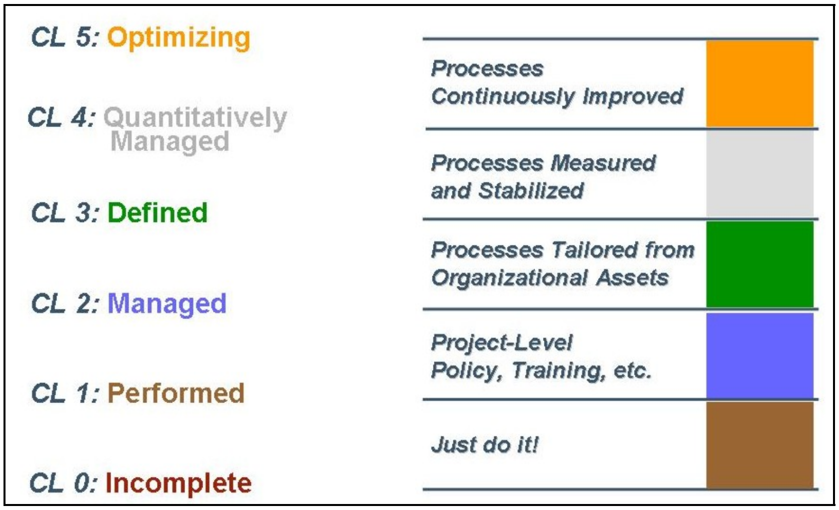
CL 5: Optimizing
CL 4: Quantitatively Managed
CL 3: Defined
CL 2: Managed
CL 1: Performed
CL 0: Incomplete
Processes Continuously Improved
Processes Measured and Stabilized
Processes Tailored from Organizational Assets
Project-Level Policy, Training, etc.
Just do it!

Figure 2—Capability Levels (CL) for Risk Management in the CMMI RSKM Process Area

What Makes CMMI RSKM Different from other Risk Management Standards?

Appraisal Method. The SCAMPI appraisal framework permits reasonably objective and repeatable assessment of the extent to which projects within an organization and between different organizations comply with the practices at CL 1 through 3—the "compliance-oriented" capability levels. This method has proven to be robust, and by forcing lead appraisals to confront the issues that arise from the appraisals, and by providing a feedback mechanism to the community, it eventually allows corrections to be made to the model based on real-world experience.

Training. The overall CMMI infrastructure includes comprehensive and formal training of practitioners, instructors, and lead appraisers. This helps assure that interpretation of the standards implicit in the model will be consistent across the community.

Levels. The capability levels themselves distinguish CMMI RSKM from other risk management standards. These allow three clear levels (CL1-3) of how "compliant" a project and organization are with the model/standard, requiring greater support from the organization as a whole as capability levels increase. At CL4 and CL5 the possibility of actually measuring and improving the *effectiveness* of the organization's risk management processes emerges.

Having said this, it must be acknowledged that CL1 is not qualitatively different from the requirements of any other risk management standard, that CL2 and CL3 concern themselves with how risk management *processes* are managed rather than how *risks* are managed, and that CL3 can be attained by simply doing what the model says to do; i.e., without demonstrating that those practices actually do anything to manage the risks. Furthermore, while many organizations have been appraised at CL3 in RSKM, we can only find two in the world that have been appraised at CL4 or CL5 in risk management. It is not a place that many organizations are inclined to go, so far.

Who Polices Gaps, Conflicts, and Overlaps, between CMMI RSKM and Other Risk Management Standards?

To my knowledge, no one does—and I believe no one should.

What Should INCOSE Do?

What INCOSE should *not* do is to try to police the gaps, conflicts, and overlaps. INCOSE lacks the broad-based common vision of risk management to be able to arbitrate the issues, or to provide a better alternative. Further, INCOSE lacks the power to impose its will on the community of project management and systems engineering practitioners who care about putting risk management practices in place.

What I believe INCOSE should do is to decide on an existing risk management standard to support, and to take on the role of being an influencer of that standard. I believe that the CMMI RSKM process area is the right standard to support. It can be supported without necessarily buying into the entire CMMI model—it can be applied by itself, or with the support of a few selected CMMI process areas. It has the training and appraisal infrastructure to give it consistency and "teeth." Finally, it has broad and visible DoD and industry support.

BIOGRAPHY

Ray Williams is currently Carnegie Mellon SEI's lead for Risk Management. He is one of the six authors of the SEI's Continuous Risk Management Guidebook (published August 1996), and also helped finalize the RSKM process area for CMMI. He is an authorized instructor for the *Introduction to CMMI* course, having taught it over a dozen times, and this helps keep him current on the CMMI model as a whole.

Mr. Williams is a member of the INCOSE RWMG and VP of Administration of the PMI's Risk Management Specific Interest Group (RiskSIG). He teaches a graduate-level course in "Risk Management for Software Intensive Projects" in Carnegie Mellon's School of Computer Science.