

A Path to Convergence of Risk Management Standards

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

Copyright © 2006 by Garry J. Roedler
Lockheed Martin Corporation
Contact: garry.j.roedler@lmco.com
Published and used by INCOSE with permission.

Currently in the area of risk management, there is no shortage of standards and guidelines containing process requirements and guidance. One of the difficulties is that this large body of information has grown in an uncoordinated manner, leading to some significant inconsistencies. This divergent growth of standards and guidelines in risk management has resulted in there being no approach and terminology that is recognized as the industry standard.

A Precedent for Convergence. In the area of measurement, there has been a very good example of a coordinated effort to establish consistent process definition, guidance, and terminology to drive convergence in the industry. This has resulted in consistent measurement standards, guidance, and models. In this situation, alliances were established between organizations, such as the Practical Software and Systems Measurement (PSM) project team, the International Council on Systems Engineering (INCOSE), the Capability Maturity Model Integration (CMMI) project team, ISO/IEC JTC1/SC7 – Software and Systems Engineering, and the Institute for Electrical and Electronics Engineers (IEEE). Over time, through good coordination and cooperation, the desired convergence has been witnessed to a great extent. All of the parties have agreed to the same measurement approach, activities, tasks, and terminology, which have been used in their respective products as follows:

- ISO/IEC JTC1/SC7
 - ISO/IEC 15939, Measurement – standard with measurement information model
 - ISO/IEC 15288, System Life Cycle Processes – Measurement activities
 - ISO/IEC 12207, Software Life Cycle Processes – Measurement process
 - ISO/IEC 16085, Risk Management – consistent measurement references
- IEEE
 - IEEE Adoption of ISO/IEC 15939
- CMMI
 - Measurement & Analysis Process consistent with PSM and ISO
- PSM
 - PSM Guide – original definition of the measurement approach
- INCOSE
 - SE Measurement Primer – consistent process and terms
 - Provided SE input for PSM guide and reviewed CMMI M&A process area

This establishes a precedent and approach to achieve convergence in an area of the project and technical processes. Currently, there is no apparent party leading any widespread effort to determine the conflicts, gaps and redundancies between standards and guidelines in risk management. Although, within ISO/IEC JTC1/SC7 and IEEE, there is an effort to align the risk management requirements and terminology for ISO risk management standards and guidelines. The cooperation between these two parties resulted in the creation of ISO/IEC/IEEE 16085:2004, which replaced IEEE Std 1540. To fully meet the alignment objective, a revision was initiated to align it with other ISO standards/guides on risk management, such as ISO Guide 73, Risk Management Vocabulary and to ensure its applicability to systems. In turn, this has influenced the Risk Management process in the current revisions to the systems and software engineering life cycle process standards for information technology (i.e., 15288 and 12207). This successful coordination of activities on risk management has also been done by "sharing" project leaders/members among the standards. For risk management, this level of coordination among project leaders sets a new precedent. This type of coordination needs to be expanded to be further reaching across the set of industry standards.

A Path to Convergence. INCOSE can and should adopt a leadership role to promote convergence in Risk Management across the industry standards and models. The challenge here will be trying to span the independent industry and domain standards and guidance. Since INCOSE does not produce standards, it can serve as an unbiased leader to facilitate a convergence effort that goes well beyond ISO and IEEE. Risk management is generally considered both a program management and a systems engineering process. In order to be able to influence the program management community for this convergence, it would be prudent to establish a collaborative approach with the Program Management Institute (PMI).

The risk management process defined in the ISO/IEC standards is general enough, yet complete enough to be applicable to both engineering and management. ISO/IEC 16085, Risk Management, defines the terminology, process requirements, activities, tasks, and application in the life cycle. This standard defines risk management as a “continuous process for systematically addressing risk throughout the life cycle of a product or service.” Although the application of this standard is focused on risk management for systems and software engineering, the process could be applied to any discipline or domain. The process consists of six activities as follows:

- a) Plan and implement risk management
- b) Manage the project risk profile
- c) Perform risk analysis
- d) Perform risk monitoring
- e) Perform risk treatment
- f) Evaluate the risk management process

Since this standard originated from IEEE Std 1540, it has been successfully battle-tested.

The same activities exist in many other risk management references, although there may be slight terminology differences. Within the ISO/IEC community, the same process, activities, tasks, and definitions are being incorporated into the revisions to the following ISO/IEC standards:

- ISO/IEC 15288, System Life Cycle Processes

- ISO/IEC 12207, Software Life Cycle Processes
- ISO/IEC 24748, Life Cycle Process Concepts and Definitions

The internal convergence efforts in ISO can be leveraged as a catalyst for a more widespread industry convergence. ISO/IEC 15288 and ISO/IEC 12207 have become the dominant standards for systems and software engineering processes. In addition, 16085 is being balloted by IEEE as an IEEE standard. With some leadership by INCOSE to establish a long-term plan for industry convergence using the ISO/IEC risk management process requirements as a baseline, the confusion from the myriad of risk management standards can be reduced. We can start the effort through achieving alignment of the INCOSE SE Handbook with this set of standards. Then systematically work on the myriad one at a time.

An Essential Relationship Not to be Overlooked. Risk management is most effective when it is integrated with the measurement process. The measurement process needs to work in conjunction with the risk management activities and tasks to help characterize and quantify risks, as shown in Figure 1. Identified risks feed into the Plan Measurement activity as information needs to be used in defining measures for further analysis. In the Perform Measurement activity, analysis of measures of process, product, and progress performance identify potential new risks to be addressed. Effective measurement can help identify risks earlier in the lifecycle to avoid growth in risk exposure. The ongoing measurement analysis also provides essential insight into risk management effectiveness.

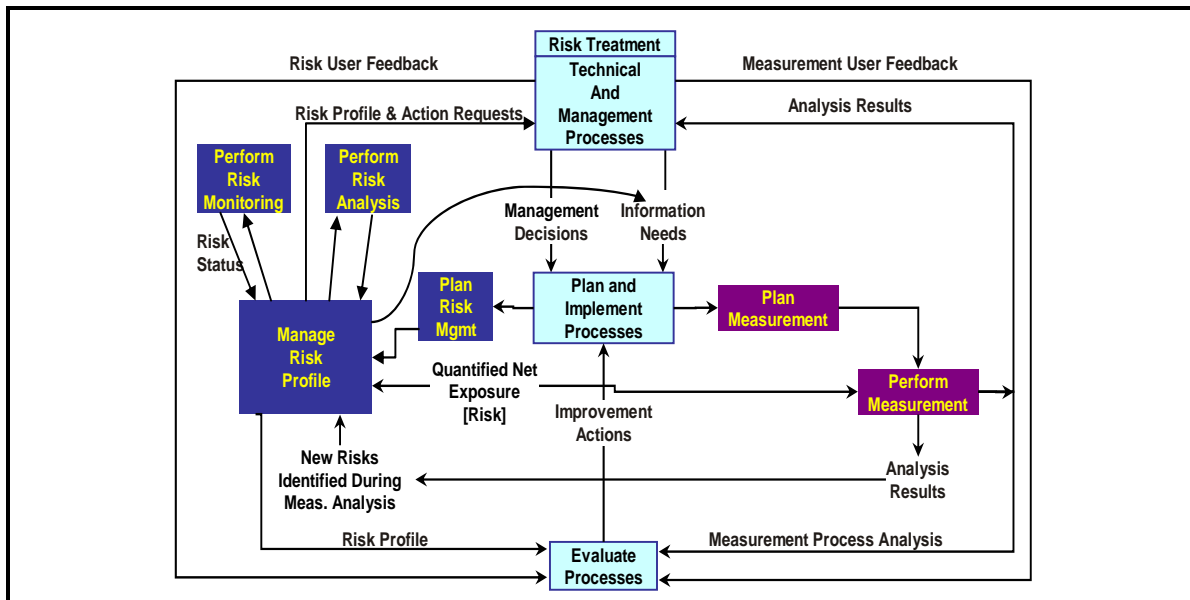


Figure 1: Measurement Relationship to Risk Management

As part of the convergence effort, INCOSE should promote the need to evolve the processes together. In ISO/IEC, this is being done. ISO/IEC 15939, defines a measurement process applicable to all engineering and management disciplines. It works in conjunction with the risk management activities and tasks defined in ISO/IEC 16085.

Biography

Garry Roedler is the Senior Manager of Systems Engineering (SE) at the Lockheed Martin Engineering Process Improvement Center. In this position, he is responsible for the development of systems engineering processes, implementation assets, and training, as well as the selection of systems engineering tools for the corporation. Previously, he was the Engineering Process Integration Manager for LM Integrated Systems & Solutions and the Systems Integration Process Review Board Chair for LM Management and Data Systems (M&DS), focusing on process improvement and achievement/sustainment of Level 5 CMM/CMMI objectives. Under his leadership, the Systems Integration organization of M&DS became the first and only organization in the world to achieve Level 5 ratings in the SE-CMM. Garry was one of the authors of the Integrated Engineering Process (LM-IEP), the Integrated Measurement Guidebook and the Risk/Opportunity Management Handbook for Lockheed Martin.

Other work includes leadership roles in various technical and standards organizations, including: US Head of Delegation and Task Group leader for ISO/IEC JTC1/SC7 Working Group 7 (software and systems engineering process standards), Practical Software and Systems Measurement (PSM) Technical Steering Group; International Council On Systems Engineering (INCOSE) Corporate Advisory Board, Technical Board and Committees; INCOSE Delaware Valley Chapter, for which he was a co-founder; the IEEE Standards Association; and the Lean Aerospace Initiative (SE Leading Indicators). Garry has worked on the author teams of several currently used standards, including ISO/IEC 15288, Systems Life Cycle Processes; ISO/IEC 15939, Measurement; ISO/IEC 16085, Risk Management; IEEE 1540, SW Risk Management.