Risk Management Maturity Level Model

Article Author: David C. Hall
                        Senior Risk Manager
                        SRS Risk Management Services

Date: 12 August 2002

Abstract

Organizations wishing to implement a formal approach to risk management or to improve their existing approach need a framework against which to benchmark their current Risk Management practice. "Best Practice" benchmarks are usually defined in terms of maturity, normally reflecting increasing levels of sophistication together with other features. This paper describes a Risk Management Maturity Model (RMMM) with four levels of capability maturity, each linked to specific attributes. Organizations and projects can use this model to assess their current level of Risk Management capability maturity, identify realistic targets for improvement, and produce action plans for developing or enhancing their Risk Management capability maturity level. This is a maturity model that is very simplified and designed to quickly target weaknesses but NOT to be so formal that it would become a constraint or overly invasive. The developers decided that an assessment of Risk Management capability did not require that much formality. If someone felt such formality was required, they could use the full EIA/IS 731 assessment process or the CMMI assessment process. All that is advocated and presented here is a simple assessment tool that helps organizations understand the maturity and possible shortcomings of their risk management process.

Introduction

Risk Management is defined as "the systematic process of identifying, analyzing, and responding to enterprise or project risk." Successful projects have dealt effectively with all types of risk[1], maximizing benefits while minimizing uncertainty. However, Risk Management still remains more of an art than a science. Several Professional Organizations and numerous individual practitioners have joined together[2] to develop guidelines and standards to define "Suggested Practices[3]" for effective Risk Management. Risk Management within organizations and individual projects needs to develop into an accepted discipline, with its own language, techniques, procedures and tools. The value of a proactive formal structured approach to managing risks and uncertainty is widely recognized, and many organizations are seeking to introduce risk management into their organizational and project processes in order to gain the potential benefits.

---

[1] See Program Report URP-001, Universal Risk Project Final Report.

[2] The formal collaboration consists of the INCOSE Risk Management Working Group, the PMI Risk Significant Interest Group, the APM Risk Significant Interest Group, the PM Risk Community of Practice and over 150 individual participants in 14 countries.

[3] We use the term "suggested practices" rather than "best practices" since all organizations, projects and operations have differing requirements and, for risk management, one size does not fit all. Considerable tailoring may have to be accomplished in most or all of the procedures and techniques described here.

Despite this increasing consensus on the value of risk management, effective implementation of risk management processes in organizations and projects is far from common. Those who have tried to integrate risk management into their business processes have reported differing degrees of success, and some have given up the attempt without achieving the potential benefits. In many of these uncompleted cases, it appears expectations were unrealistic, and there was no clear vision of what implementation would involve or how it should be managed. ***Organizations attempting to implement a formal structured approach to risk management need to treat the implementation itself as a project, requiring clear objectives and success criteria, proper planning and resourcing, and effective monitoring and control.*** In order to define the goals, specify the process and manage progress, it is necessary to have a clear view of the organization's current approach to risk, as well as a definition of the intended destination. The organization must be able to benchmark its present maturity and capability in managing risk, using a generally accepted framework to assess current levels objectively and assist in defining progress towards increased maturity.

There is currently a broad consensus on the fundamentals and potential benefits of project risk management when it is conducted within a mature and effective process and supported by a comprehensive infrastructure. The core elements of project risk management are known and used, and many organizations are noting the benefits of implementing risk processes within their projects and wider business. However, there are a number of areas where risk management needs to develop in order to build on the foundation that currently exists. One of the most important of these is the ability to measure effectiveness in managing risk.

Risk Management Maturity Model

The Risk Management Maturity Model (RMMM) outlined in this article focuses on Risk Management specifically and provides a less formal methodology that can be accomplished much easier than a formal assessment. It is more of a generic risk-focused maturity model that attempts to be of assistance to organizations wishing to implement formal risk processes or to improve their existing approach. It should be applicable to all types of projects and all types of organizations in any industry, government or commercial sector.

The RMMM has been designed as a diagnostic tool instead of a prescriptive model for implementation. The authors of this report recommend that organizations use either EIA/IS-731.1 or CMMI – SE/SW for a formal administrative system if one is desired. The RMMM offers a framework to allow an organization to benchmark its approach to risk management against four standard levels of maturity, and outlines the activities necessary to move to the next level. It provides clear guidance to organizations wishing to develop or improve their approach to risk management, allowing them to assess their current level of maturity, identify realistic targets for improvement, and develop action plans for increasing their risk maturity. While too lengthy and detailed for this article, the final report on the RMMM details the four maturity levels and provides guidelines to allow a diagnosis of your organization's current maturity level. The report also notes that different barriers are faced by organizations at each of the RMMM levels, which must be

overcome if progress is to be made to the next level of risk maturity. These barriers are outlined together with some suggested strategies for overcoming them.

The Risk Management Maturity Model Framework
The maturity of an organization's Risk Management processes can be categorized into groups that range from having no formal process to fully integrated into all aspects of the organization. In order to reflect this, the Risk Management Maturity Model described in this article (and more fully in the final report) provides four standard levels of risk management maturity (Figure 1). As with all models, it is expected that some organizations may not fit neatly into these categories, but the RMMM levels are defined sufficiently different to accommodate most organizations unambiguously. It was felt that to have more than four levels would increase ambiguity without giving any additional refinement to the model.
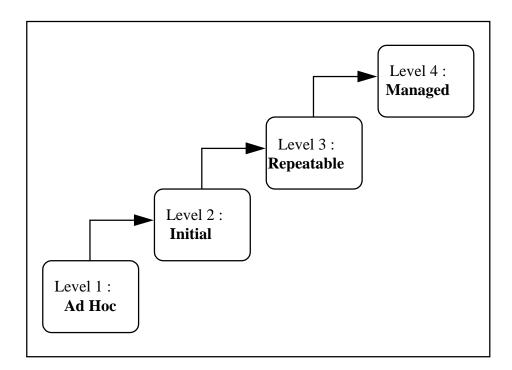

Figure 1 : The Four Levels of Risk Management Maturity

Level 1 – Ad Hoc (Worship The Hero)
At the Ad Hoc Level, the organization is unaware of the need for risk management and has no structured approach to dealing with uncertainty, resulting in a series of crises for each project or operation.

Level 2 – Initial (Try It Out)
At the Initial Level, organizations are experimenting with the application of risk management, usually through a small number of nominated individuals within specific projects.

Level 3 - Repeatable (Plan The Work, Work The Plan)
At the Repeatable Level, the organization has implemented risk management into their routine business processes and implements risk management in most, if not all, projects.

Level 4 - Managed (Measure The Work, Work The Measures)
At the Managed Level, the organization has established a risk-aware (not risk-averse) culture that requires a proactive approach to the management of risks in all aspects of the organization.

Table 1 presents one set of the attributes of a typical organization at each RMMM level under four attribute headings: *Culture, Process, Experience* and *Application*. The full breakout contained in the final report enables an organization to compare itself against clear criteria which have been accepted by numerous professional Risk Management organizations and assess its current level of risk maturity. It is recognized that some organizations may cross the boundaries between successive RMMM levels, but the granularity between levels is such that there should be a clear distinction in most cases and it should prove possible to determine where most organizations are in relation to a single level.

The extent to which the attributes noted in the Maturity Level Table are implemented at each level determines the process maturity level rating of an organization. The extent of implementation of a specific attribute is evaluated by assessing:
- Commitment to perform (policies and leadership)
- Ability to perform (resources and training)
- Activities performed (plans and procedures)
- Measurement and analysis (measures and status)
- Verification of implementation (oversight and quality assurance)

Table 1. Example Model Attributes – One Set

Attribute	Level 1 – Ad Hoc	Level 2 – Initial	Level 3 - Repeatable	Level 4 - Managed
Definition	Unaware of the need for management of uncertainties (risk).	Experimenting with risk management through a small number of individuals.	Management of uncertainty built into all organizational processes.	Risk-aware culture with proactive approach to risk management.
Culture	No risk awareness.	Risk management used only on selected projects.	Accepted policy for risk management.	Top-down commitment to risk management, with leadership by example.
Process	No formal process.	No generic formal processes	Generic processes applied to most projects.	Risk-based organizational processes.
Experience	No understanding of risk principles or language.	Limited to individuals who may have had little or no formal training.	In-house core of expertise.	All staff risk aware and capable of using basic risk skills.
Application	No structured application.	Inconsistent application of resources.	Routine and consistent application to all projects.	Risk ideas applied to all activities.

Conclusions
The implementation of risk management in an organization is not a minor challenge, and cannot be undertaken in a short period of time. Risk Management is not a simple process of identifying techniques, sending personnel to training courses, buying software and

getting on with it. Risk management capability is a broad spectrum, ranging from the occasional informal application of risk techniques to specific projects, through routine formal processes applied widely, to a risk-aware culture with proactive management of uncertainty.

The Risk Management Maturity Model outlined in this article allows organizations to benchmark their risk management capability against four standard levels of maturity. It also allows organizations to identify what needs to be done in order to improve and increase their ability to manage risk. Use of the RMMM will also enable customers, suppliers and other areas of the organization to determine how well a project or organization is implementing risk management, and can aid in the development of specific strategies for going to a higher maturity level. Some additional work is required to enhance the diagnostic elements of the RMMM; however, the present RMMM framework provides a useful tool to those organizations or projects interested in either implementing a formal approach to risk management or improving their existing approach.

Anyone wishing to obtain a copy of the Risk Management Maturity Model final report, please contact the following:

Contact Information:
David C. Hall   Phone: 301-641-1530
Senior Risk Manager   e-mail: halld105048@yahoo.com
SRS Risk Management Services
6301 Ivy Lane, Suite 516
Greenbelt, Maryland 20770 USA
web site: http://www.msd.srs.com/service-proriskman.htm