Risk Management Maturity Level Development

April 2002

Risk Management Research and Development Program Collaboration

[Formal Collaboration:
INCOSE Risk Management Working Group; Project Management Institute Risk Management Specific Interest Group; UK Association for Project Management Risk Specific Interest Group]

Table of Contents

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 report 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 we advocate and present here is a simple assessment tool that helps organizations understand the maturity and possible shortcomings of their risk management process.

Major Contributors

Roger Graves, Davion Systems Ltd [rgraves@davion.com]
Dr. Stephen Grey, Broadleaf Capital [grey@broadleaf.com.au]
Scott Gunderson, TriQuint Semiconductor [sgunderson@tqs.com]
David C. Hall, SRS Information Services [dhall5@earthlink.net]
Dr. David Hillson, PM Professional [dhillson@pmprofessional.com]
Dr. David Hulett, Hulett & Associates [info@projectrisk.com]
Robert Jones, Robert Jones Associates [RJonesAssn@aol.com]
Ron Kohl, Titan Sytems [ron.kohl@titan.com]
Steve Waddell, Naptheon [waddell_js@naptheon.com]

Additional Reviewers

Note that inclusion on this list does not imply agreement with the contents of this report.

Bruce Chadbourne
Paul Callender
Ralph Simon
Craig Peterson
Elmar Kutsch
Sandee Whitmoyer
Ted Hammer
David Jacobs
Etienne Bossard
Ron Siddaway
Christopher Boedicker

1.0 Introduction

The *PMBOK® Guide* – 2000 Edition, defines Project Risk Management as "the systematic process of identifying, analyzing, and responding to project risk." Successful projects have dealt effectively with all types of risk[1], maximizing benefits while minimizing uncertainty. This Program is developing guidelines and standards to define "Suggested Practices[2]" for effective Risk Management. Risk Management within organizations and individual projects has developed 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.

Despite this increasing consensus on the value of risk management, effective implementations of risk management processes into organizations and projects are not 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 that 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.

This report describes a Risk Management Maturity Model (RMMM) with four levels of process maturity, each linked to specific attributes, that provides a methodology that allows an organization to determine whether or not its risk processes are adequate for the

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

[2] 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.

organization[3], identify realistic targets for improvement, and produce action plans for developing or enhancing their Risk Management process 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 organizational and project Risk Management processes did not require much formality. If an organization believed that such formality was required, they can use the full EIA/IS 731 assessment process (see appendix 1) or the CMMI assessment process. This model provides some measures to enable an organization to compare its risk management process with Suggested Practice and an accepted benchmark for determining your organizational risk management process maturity level. Note that much of the model is based on the initial work accomplished by Dr. David Hillson as detailed in references 1 and 2.

2.0 The Risk Management Maturity Model (RMMM)

The concept of maturity models is well developed and accepted. The Software Engineering Institute (SEI) at Carnegie-Mellon University has developed a Capability Maturity Model (CMM) for Software organizations and one (CMMI) for Systems Engineering organizations[4]. These models define five levels of increasing capability and maturity, termed Initial (Level 1), Repeatable (Level 2), Defined (Level 3), Managed (Level 4) and Optimizing (Level 5). Each level is clearly characterized and defined, enabling organizations to assess themselves against an agreed scale. Having discovered its CMM level, an organization can then set clear targets for improvement, aiming towards the next level of capability and maturity.

Although the SEI CMMI is becoming well established, its application is limited by its overall invasiveness. To fully apply the CMMI model (which contains a risk management maturity model) requires significant amounts of resources and integration within the overall Systems Engineering process. The RMMM outlined in this report focuses on Risk Management specifically and provides a less formal methodology that can be accomplished much easier than a formal CMMI 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 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 is designed as a diagnostic tool instead of a prescriptive model for implementation. The authors recommend that organizations use either EIA/IS-731.1 or CMMI – SE/SW for a formal administrative system if one is desired. The RMMM

[3] Note that there can be (and usually are) differing issues (attribution of the importance of a risk occurring is normally the one most seen) between an organization and an individual project. This fact needs to be taken into account in using the model. One must first decide if they want to determine their ***organization's*** risk management maturity level or a specific ***project's*** risk management maturity level.

[4] www.sei.cmu.edu/cmmi

includes four levels to measure maturity, which compare to other model levels as shown in the following table:

Table 1. Comparison of Maturity Model Levels

Level	**RMMM**	**CMMI – SE/SW**	**EIA/IS-731.1**
0	*Ad Hoc*	Incomplete	Initial
1	*Initial*	Performed	Performed
2	*Repeatable*	Managed	Managed
3	*Repeatable*	Defined	Defined
4	*Managed*	Managed quantitatively	Measured
5	*Managed*	Optimizing	Optimizing

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. The Risk Management Maturity Model (RMMM) described here 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. The four RMMM levels are outlined, followed by guidelines to allow diagnosis of current level. Suggested strategies for developing towards the next level of maturity are then discussed.

3.0 The Risk Management Maturity Model Framework

The maturity of an organization's Risk Management processes can be categorized into groups that range from those who have no formal process to organizations where risk management is fully integrated into all aspects of the organization. In order to reflect this, the Risk Management Maturity Model (RMMM) described in this 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.

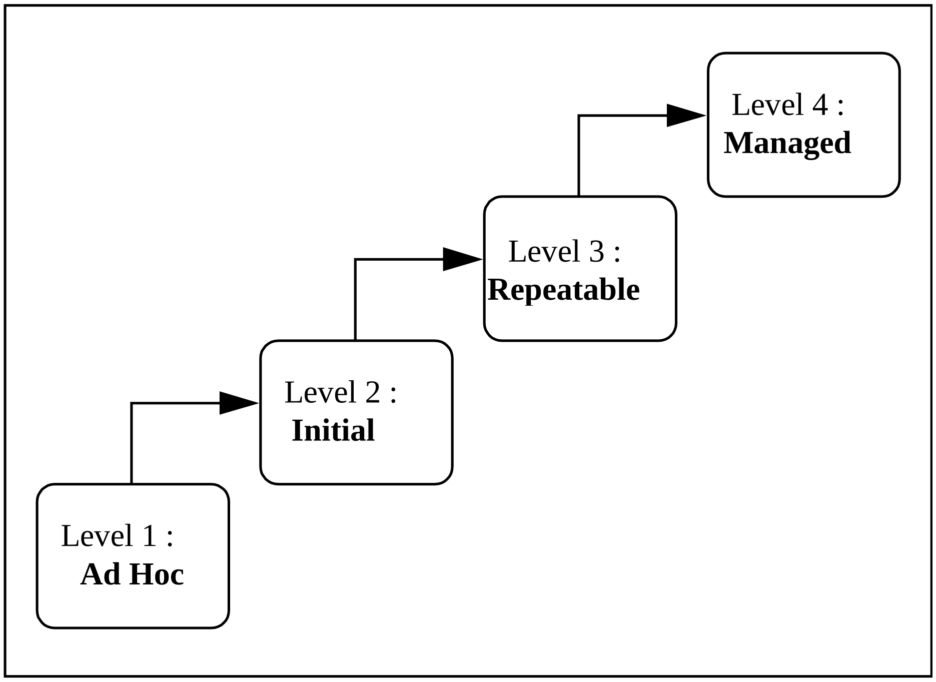

Figure 1 : The Four Levels of Risk Management Maturity

The RMMM levels are described as follows:

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[5] or operation. Management and engineering processes, if they exist, are repetitive and reactive, with little or no attempt to learn from past projects or to prepare for future uncertainties. No attempt is made to identify risks to the project or to develop mitigation or contingency plans. The normal method for dealing with problems is to react after a problem occurs with no proactive thought. During a crisis, projects typically abandon plans and hope for the best. Project success depends on having an exceptional manager and a seasoned and effective team. Occasionally, capable and forceful managers can identify and work to mitigate risks during the project; but when they leave, their influence leaves with them. Even a strong engineering process cannot overcome the instability created by the absence of sound risk management practices.

In spite of this chaotic process of reactive crisis management, Level 1 organizations frequently develop products that work, even though they will normally exceed their original budget and schedule and will not contain all of the originally required functionality. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent

[5] For this discussion, the term "project" is defined as a temporary endeavor undertaken to achieve a particular aim for an identified customer. Every project has a definite beginning and a definite end. While projects are similar to operations in that both are performed by people, both are generally constrained by limited resources, and both are planned, executed and controlled, projects differ from operations in that operations are ongoing and repetitive while projects are temporary and unique. Projects are created at all levels of an organization. They may involve a single person or thousands. Their time spans vary greatly. They may involve a single department of one organization or cross organizational boundaries.

individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

Note that the most difficult step in this maturity model is the move from Level 1 to Level 2. This is because of all the management procedures and activities that have to be put in place. It can also be due to the lack of perceived need to change. An Ad Hoc organization may lack any sense or awareness of having a problem. At higher levels of maturity the organizational and project management has better visibility on the uncertainties, and can take any necessary mitigative or contingency actions. This visibility enables management to take such action before something goes wrong or to have a plan in place when something goes wrong. The difference in maturity levels is also characterized by the ability to accurately identify and proactively deal with uncertainties. As an organization moves up the maturity level ladder, identification of risks becomes more accurate and the mitigation/contingency actions required become clearer.

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. At this level, the organization has no formal or structured Risk Management process in place. Although the organization is aware, at some level, of the potential benefits of managing their project risks, there is no effectively implemented organization-wide process implemented. Some projects, those containing the nominated individuals, learn from past mistakes, however, there is no method implemented for providing these Lessons Learned to all of the organization's projects. Risk management at this point may be described as the start of crystallization of the organization's corporate experience. The organization is becoming aware that it can learn from past mistakes, but this knowledge is not yet formalized nor are there any structures in place to ensure its consistent application throughout the organization.

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. Generic risk policies and procedures are formalized and widespread, and the benefits are understood at all levels of the organization, although they may not be consistently achieved in all cases. Planning and managing new projects is based on experience with similar projects. Risk Management capability is enhanced by establishing basic Risk Management discipline on a project-by-project basis. Projects implement risk management through processes that are defined, documented, practiced, trained, measured, enforced, and improvable. All projects have an assigned Risk Manager. On small projects, the roles of the Project Manager and Risk Manager may be combined in the same person, but on larger projects the Risk Manager is distinct from the Project Manager.

Projects in Level 3 make realistic project commitments based on the results observed on previous projects and on the risks identified for the current project. The Risk Manager for a project track costs, schedules, functionality and quality[6]; problems in meeting commitments are identified as they arise. The Risk Manager for the project works with its customers and subcontractors (if any) to establish an effective customer-supplier relationship.

Risk Management processes may differ between projects in a Level 3 organization. The organizational requirement for achieving Level 3 is that there be organization-level policies that guide the projects in establishing the appropriate management processes. The risk management capability of Level 3 organizations can be summarized as disciplined because planning and tracking of the project is stable and earlier successes can be repeated. The project's risk management process is under the effective control of a project management system, following realistic plans based on the performance of previous 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. Risk information is continually developed and actively used to improve all organization processes and to increase the probability of success in projects and operations. A standard Risk Management process (or processes) is documented and used across the organization. Processes established at Level 3 are used (and changed, as appropriate) to help the organization’s project and operations managers and technical staff perform more effectively. A group of personnel within the organization are assigned responsibility for Risk Management. This formal assignment provides for an informal communications channel to organization management outside of the Project communications channels or operational management structure. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles.

Projects tailor the organization's standard Risk Management process and tools to develop their own defined process, which accounts for the unique characteristics of the project. It is the process used in performing the project's activities. A defined risk management process contains a coherent, integrated set of well-defined risk identification, assessment, handling and monitoring tools and processes. A well-defined process can be characterized as including readiness criteria, inputs, standards and procedures for performing the work, verification mechanisms (such as peer reviews), outputs, and completion criteria. Because the risk management process is well defined, management has good insight into risks and their potential impact on the project or operation.

The Risk Management process capability of Level 4 organizations can be summarized as standard and consistent because activities are stable and repeatable. Within established product lines, cost, schedule, functionality and quality risks are known, controlled, and risk mitigation status is tracked. This process capability is based on a common,

[6] Note: The effect of a risk occurring can be to deliver lower quality, both in the project deliverables (e.g. more bugs in a software program) and in the project process itself (e.g. more accidents on a construction site). Quality is as important a measure of project success as the delivered functionality.

organization-wide understanding of the activities, roles, and responsibilities in a defined risk management process.

Innovations that exploit the best risk management practices are identified and transferred throughout the organization. Risk Management teams in Level 4 organizations continuously analyze the results from past projects to determine how accurate risk identification was versus actual impacts and causes. They disseminate lessons learned throughout the organization.

4.0 Determining Organizational Maturity Level

The brief descriptions of each RMMM level can indicate where an organization stands in terms of the relative maturity of its risk processes, but a more detailed diagnostic tool is required for objective and consistent assessment of risk management process maturity.

Table 1 (Appendix 1) presents suggested attributes of a typical organization at each RMMM level under four attribute headings: ***Culture, Process, Experience*** and ***Application***. This breakout enables an organization to compare itself against clear criteria that have been accepted by numerous professional Risk Management organizations[7] 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 to a single level.

The extent to which the attributes noted in the Maturity Level Table in Appendix 1 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)

5.0 Progressing Between Maturity Levels

The assessed RMMM level can be used in a number of ways. For example, organizations may wish to enhance their level of risk capability by devising strategies to enable more effective management of risk. Alternatively, they may want to rate themselves against key competitors in order to gain advantage in the market place.

Once your current risk maturity level is determined, action plans for moving towards the next level can be developed. Many organizations are at Level 2 or Level 3, or have

[7] International Council on Systems Engineering Risk Management Working Group, Project Management Institute Risk Management Specific Interest Group and the Risk Management Specific Interest Group of the UK Association for Project Management.

embarked on the transition from Level 2 to Level 3 and a significant number are at Level 1.

Different barriers are faced by organizations at each of the RMM levels, which must be overcome if progress is to be made to the next level of risk maturity. These are outlined below, together with some suggested strategies for overcoming them.

Level 1 to 2 – Ad Hoc to Initial

The Level 1 organization faces a number of problems as it starts implementing effective risk management:

- Initially there is no clear understanding of a formal risk management process, procedures and techniques, and even the language and terminology will be unknown.
- There is no clear concept of the benefits that can be gained from formal risk management, and the cost of implementing the process is normally not considered.
- There is no in-house expertise or experience in performing risk management or when trying to consider the applicability of risk management to the organization' programs and business processes.
- At least some of the organization's projects and business processes are in crisis at any given time, leading to a lack of time, energy or resources to commit to installing and following a new process.
- The organization's upper level management may not be receptive to anyone, internal or external, that is promoting risk management, since they are uninformed customers and lack any track record or yardstick against which to judge the promised benefits. They may also believe that acknowledging that the organization's processes and projects are subject to uncertainty may be seen as an admission of weakness or lack of skill.
- The organizational culture may not be committed to quality and may lack the concept of professionalism.

In order to develop from an **Ad Hoc** level to the **Initial** level, a number of actions must be accomplished. Some of these actions are as follows (in no specific order):

- Clearly define the objectives of the risk management implementation to enable the risk process to be tailored and scoped accordingly.
- Get advice and guidance from recognized external experts who have a track record in assisting organizations in this type of implementation. Such external experts should be selected carefully, and the organization should beware of being encouraged to adopt a generic solution that does not match their particular requirements.
- Identify specific personnel to be the original implementers, carefully select and build a prototype team.
- Ensure adequate training and support for this team, including all the necessary risk skills and techniques, to ensure that they can act as "intelligent customers".
- Undertake awareness briefings to sell the vision of risk management and its potential benefits to the entire project organization, from senior management to front-line employees. These awareness briefing should include project customers

and subcontractors (see appendix 2 for some insight into views on risk management one is likely to encounter when accomplishing this action).

- Ensure corporate backing, with nomination of a senior management sponsor to promote the implementation process.
- Nominate pilot applications for risk management, carefully selected to maximize the chances of early success.
- Publicize and celebrate successes. Seek to develop momentum in the risk process and to encourage other projects and individuals to apply risk management to their areas as they see clear benefits.
- Plan for the long-term, recognizing that effective implementation of risk management will not be achieved overnight. Count the cost of the implementation project, and ensure commitment of the necessary resources before starting.
- Build effective controls into the process from the outset, with breakpoints to enable progress to be monitored and reviewed at key intervals. Collect and trend appropriate metrics.
- Consider producing draft risk procedures with templates for key inputs and outputs.
- Identify and use appropriate project risk management tools such as risk information databases.

Level 2 to 3 – Initial to Repeatable

A Level 2 organization has a number of individuals (possibly only one) able to effectively plan and apply risk management procedures and techniques. At this level, risk management is seen as an additional activity to be undertaken where necessary. So whatever risk process is used by various projects is unlikely to be used consistently or widely. Application of any risk management process is limited to a few major or significant projects.

This introduces a number of barriers to be overcome to reach Level 3 and normalize the application of a risk management process across the organization. It should be noted here that that some organizations may choose to remain at Level 2, with risk management being undertaken by an in-house team on selected projects only. There is nothing wrong with this approach. The transition to Level 3 should only be undertaken if the benefits are worth the cost and effort involved.

Some of the problems faced by the Level 2 organization attempting to progress to Level 3 are as follows:

- Lack of organizational-wide formal risk processes produces inconsistency in their application and inconsistency in results.
- Dependence on the skills of a few in-house staff could limit the overall effectiveness of the risk process and negatively impact both existing projects that use risk management and projects attempting to implement the process for the first time..
- Lack of support for those implementing risk management may lead to disillusionment and low morale.
- Limiting promotion of risk to the lone enthusiast can undermine the credibility of the risk process.

- Partial or inconsistent application of risk processes is unlikely to generate useful metrics that fully demonstrate the benefits of managing risk. There is therefore no auditable track record of what risk management can achieve, resulting in a lack of credibility and a reluctance to adopt risk management more formally.
- Poor use of risk assessment tools and risk information databases.
- Lack of a benchmarking process to check process capability against industry standards.

These problems can be addressed in a number of ways to enable the organization to progress towards Level 3. Where the actions listed above for the Level 1 to 2 transition are not in place, these should be considered in addition to those provided below:

- Reinforce and strengthen corporate backing for those individuals and teams attempting to implement the risk management process. Visible endorsement from senior management is essential to give the necessary credibility.
- Provide formal risk training to develop in-house expertise and process knowledge.
- Use external expertise as necessary to reinforce and support existing in-house skills. Use of external expertise can be useful in extending your existing risk management process into new areas of the organization. Many of these new areas may be outside the knowledge of your in-house staff. External consultants can also be used to apply the risk management process to novel or difficult areas.
- Allocate adequate resources to the risk management implementation process, with assignment or recruitment of sufficient staff, and assigned budgets for risk management training, risk assessment tools and other required risk management activities.
- Select key projects to demonstrate the benefits of risk management in all areas of the organization's business.
- Continue to publicize and celebrate successes, encouraging wider application of risk management to other areas as benefits become clear.
- Provide opportunities for in-house staff to attend ongoing risk management training courses, conferences and seminars, workshops, etc.
- Formalize the chosen risk management process, with clear definition of the scope and objectives of risk management, together with agreed upon procedures and properly selected tools.
- Develop and promulgate an organizational policy on the use of risk management.
- Insist that your project managers use risk management as part of their routine management of projects and business processes. Include regular risk reporting as an important part of management reviews.
- Start to assemble metrics from the risk process; identification of generic risks, effective responses, the cost of risk reduction, etc. Specific checklists can be generated to facilitate the risk identification and assessment processes, based on actual experience of risk management within the organization.

Level 3 to 4 – Repeatable to Managed

Level 3 is probably sufficient for most organizations, where risk processes are integral to the organization and are consistently and routinely applied to most or all projects. However, the consensus of the professional organizations that contributed to this model was that the Risk Management Maturity Model needed to identify a level beyond Level 3, a maturity level where identifying, assessing and managing uncertainty becomes second nature and is built into all the activities and business processes of the organization. At Level 4, an organization can systematically use risk processes to address those uncertainties that have potential positive impact (i.e., opportunities or "upside risk"). In many ways the Level 3 to Level 4 change is expected to be almost as difficult as the transition from Level 1 to Level 2, since the Level 3 organization could easily come to believe that it has fully implemented risk management and no further change is needed. If the organization wishes to progress to Level 4, the following problems are likely to be encountered:

- Loss of momentum could result in failure to maintain the required standards of application, with resultant loss of quality of risk management support. This would reduce the credibility of the risk management process, making it seem to be a temporary management fad whose time has passed.
- The organization could fail to update the risk management process to take account of changes in business needs or other developments in the marketplace. This could result in the risk process becoming outdated and increasingly irrelevant to the business of the organization.
- Lack of continued investment in the risk management process could result in reduced relevance or capability, as tools become obsolete, techniques become superseded and personnel skills are not maintained.
- Development of in-house expertise might result in risk management being seen as a specialist discipline that is undertaken by experts, with consequent reduction in commitment and ownership by others in the projects and the organization.

Actions to assist in progress towards Level 4 are as follows (in no specific order):

- Ensure effective learning from experience. Undertake regular reviews of the risk management process, with value engineering of the process to ensure that it remains fully effective.
- Amend and strengthen the risk management process where necessary, including investment in new tools, new methods, personnel training, etc.
- Investigate novel applications of the risk management process beyond those already covered. Seek to modify and apply risk management to every activity within the organization.
- Use every means possible to develop a ***Risk Management Culture***, encouraging all personnel to ***think risk***, be aware of uncertainty and use risk techniques to assess and manage potential threats and opportunities. Build risk thinking into your organizational culture. Be aware of the possible range of attitudes about risk (appendix 3).
- Ensure that risk is included as a routine criterion in all decision-making.
- Identify and counter incidences of "risk fatigue", where staff are losing interest in the process or there is a potential loss of momentum. Use regular re-launch promotions to renew the process, celebrating successes, publicizing improvement metrics, and rewarding effective risk management.
- Undertake regular risk management training to ensure that skills remain current.

- Consider use of external risk expertise to widen the application of risk management into novel areas of the organization, or to add the necessary momentum to maintain progress or introduce change.

Maintaining Level 4

It is expected that to succeed in making risk management a natural part of any organizational culture will require some significant changes in determining how to apply risk techniques throughout the business and proactively manage uncertainty (including both risks and opportunities) in order to maximize the benefits mandates many changes in existing organizational cultures and personal beliefs. Since the CMM maturity levels have been available, very few organizations are at Level 5 (their top level). For many organizations, the benefits of achieving the pinnacle of maturity have not been seen as worth the cost to get there. In addition, once this pinnacle is achieved, effort (and resources) must be expended to maintain the position. A continuous improvement process is required to stay at Level 4 or any other level; without such a process it is of course possible to move down the RMMM framework and drop to a lower level or risk management capability. An RMMM Level 4 organization will be threatened by complacency and boredom and should consider a number of actions to counter these problems, including those listed below:

- Ensure continued commitment of senior management. It may be necessary or beneficial to change the sponsor from time to time to allow injection of fresh ideas and momentum.
- Use audit and review techniques to keep application of risk management techniques at the required quality and standards.
- Take full advantage of the competitive edge that results from proactive management of uncertainty (including both risks and opportunities).
- Extend risk management beyond the usual applications, pioneering its use in all areas of the business.
- Continually invest in improving the risk process, tools, techniques, personnel skills etc.
- Continue to involve customers and suppliers in the risk process.

6.0 Conclusions

The implementation of risk management into 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 (RMMM) presented in this report 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.

References

1. Towards a Risk Maturity Model, Dr. David Hillson, International Journal of Project & Business Risk Management, Volume 1, Issue 1, pages 35-45, January 1997
2. Benchmarking Risk Management Capability, Dr. David Hillson, PMI Europe 2000 Symposium Proceedings, January 2000
3. Project Management Institute. 2000. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* – 2000 Edition. Newtown Square, PA: Project Management Institute, page 127.
4. Spotlight: CMMI Model Representations, Sandy Shrum, SEI Interactive, December 1999
5. RM^3 – Risk Management Maturity Model, Steve Waddell, private communication, February 2002
6. Key Characteristics of a Mature Project Risk Management Organization, Dr, David Hulett, 13th Annual International Integrated Program Management Symposium Proceedings, 2001
7. Project Management – Risk Management: Continuous Representation, CMMI-SE/SW/IPPD/SS, version 1.1, 2001, www.sei.cmu.edu/cmmi/products/models.html
8. Software, Systems Engineering and Product Development Capability Maturity Models (CMMs), www.sei.cmu.edu/cmm/cmms/transition.html
9. Risk Management in Complex Project Organizations: A Godfather-Driven Approach, G. Getto and D. Landes, Proceedings of the 30th Annual Project Management Institute 1999 Seminars and Symposium, October 1999
10. Industry Models of Risk Management and Their Future, K. Artto and D. Hawk, Proceedings of the 30th Annual Project Management Institute 1999 Seminars and Symposium, October 1999
11. Risk and Opportunity Management, K. Forsberg and H. Mooz, Proceedings of the INCOSE Symposium, 2001.

Appendix 1 – Risk Management Maturity Level Checklist

	Level 1 – Ad Hoc	Level 2 – Initial	Level 3 – Repeatable	Level 4 - Managed
Definition	Unaware of the need for management of uncertainties (risk). No structured approach to dealing with uncertainty. Repetitive and reactive management processes. Little or no attempt to learn from past projects or prepare for future projects.	Experimenting with risk management through a small number of individuals. No structured approach in place. Aware of potential benefits of managing risk, but ineffective implementation.	Management of uncertainty built into all organizational processes. Risk management implemented on most or all projects. Formalized generic risk process. Benefits understood at all organizational levels, although not always consistently achieved.	Risk-aware culture with proactive approach to risk management in all aspects of the organization. Active use of risk information to improve organizational processes and gain competitive advantage.
Culture	No risk awareness. No upper management involvement. Resistant/reluctance to change. Tendency to continue with existing processes even in the face of project failures. Shoot the messenger.	Risk process may be viewed as additional overhead with variable benefits. Upper management encourages, but does not require, use of Risk Management. Risk management used only on selected projects.	Accepted policy for risk management. Benefits recognized and expected. Upper Management requires risk reporting. Dedicated resources for risk management. “Bad news” risk information is accepted.	Top-down commitment to risk management, with leadership by example. Upper management uses risk information in decision-making. Proactive risk management encouraged and rewarded. Organizational philosophy accepts idea that people make mistakes.
Process	No formal process. No Risk Management Plan or documented process exists. None or sporadic attempts to apply Risk Management principles. Attempts to apply Risk Management process only when required by customer.	No generic formal processes, although some specific formal methods may be in use. Process effectiveness depends heavily on the skills of the project risk team and the availability of external support. All risk personnel located under project.	Generic processes applied to most projects. Formal processes incorporated into quality system. Active allocation and management of risk budgets at all levels. Limited need for external support. Risk metrics collected. Key suppliers participate in Risk Management process. Informal communication channel to organization management.	Risk-based organizational processes. Risk Management culture permeating the entire organization. Regular evaluation and refining of process. Routine risk metrics used with consistent feedback for improvement. Key suppliers and customers participate in the Risk Management process. Direct formal communication channel to organization management.
Experience	No understanding of risk principles or language. No understanding or experience in accomplishing risk procedures.	Limited to individuals who may have had little or no formal training.	In-house core of expertise, formally trained in basic risk management skills. Development and use of specific processes and tools.	All staff risk aware and capable of using basic risk skills. Learning from experience as part of the process.

				Regular training for personnel to enhance skills.
Application	No structured application. No dedicated resources. No risk management tools in use. No risk analysis performed.	Inconsistent application of resources. Qualitative risk analysis methodology used exclusively	Routine and consistent application to all projects. Dedicated project resources. Integrated set of tools and methods. Both qualitative and quantitative risk analysis methodologies used.	Risk ideas applied to all activities. Risk-based reporting and decision-making. State-of-the-art tools and methods. Both qualitative and quantitative risk analysis methodologies used with great stress on having valid and reliable historical data sources. Dedicated organizational resources.

Appendix 2
EIA 731

Systems Engineering Capability Model (SECM) – EIA/IS 731

What is EIA/IS-731?

The G-47 Committee of GEIA sponsored project PN-3879, a joint working group composed of GEIA, EPIC, and INCOSE, to bring together the EPIC Systems Engineering Capability Maturity Model (SE CMM) and the INCOSE Systems Engineering Capability Assessment Model (SECAM) into a single capability model. The purpose was to minimize confusion within the industry and to relate the resulting capability model to the EIA-632 Standard, Processes for Engineering a System. The new capability model has been developed as EIA/IS-731, Systems Engineering Capability Model (SECM), and will be issued as an interim standard. EIA/IS 731 is published and available

History

EIA/IS-731 was selected by the CMMI Steering Group as a primary source document for systems engineering processes. EIA/IS-731, Systems Engineering Capability Model, is not a process standard but actually a standard for defining and assessing maturity of the Systems Engineering discipline. To eliminate confusion, EIA has created EIA/IS-731 as an interim standard and intends to allow EIA/IS-731 to go out of existence as the CMMI comes into existence. It is hoped that this will eliminate confusion and conflict within the systems engineering community – one of the original objectives of EIA, EPIC, and INCOSE in cooperating to create EIA/IS-731.
Reference: http://www.geia.org/sstc/G47/page6.htm

Appendix 3
Basic Risk Attitudes

From: *Benchmarking Risk Management Capability* by Dr. David Hillson, PMI Europe 2000 Symposium Proceedings, January 2000

Based on years of experience by the risk practitioners that aided in the development of this model, one thing stands out: the organization's attitude and culture can make or break the risk management efforts. The only successful ventures found are where the management team was 100% behind the effort. They backed up the commitment with people and money resources as well as leadership in making sure it was implemented. Half-hearted management support only erodes the effort in the long term and gives people a way out of using good processes. In this vein, there are three basic risk attitudes one normally runs into. They can be summarized as follows:

1. *Risk-averse*: This indicates a conservative risk attitude with a preference for secure payoffs. People who are risk-averse make good middle managers, administrators and engineers. Their key characteristics include being practical, accepting, and showing common sense. Risk-averse people enjoy facts more than theories, and support established methods of working. They excel at activities that involve remembering, persevering and building.
2. *Risk-seeking*: These show a preference for speculative payoffs, and make good entrepreneurs and negotiators. Risk-seeking people are adaptable and resourceful, enjoy life and are not afraid to take action. They are good at activities that require performing, acting and taking risks.
3. *Risk-neutral*: This attitude prefers future payoffs. People who are risk-neutral make good executives, system architects and group leaders. They think abstractly and creatively and envisage the possibilities. They enjoy ideas and are not afraid of change or the unknown. Risk-neutral people are good at learning, imagining and inventing.

The importance of understanding risk attitude is clear, since people have such a profound effect on the effectiveness of any risk process. Knowledge of potential problems in convincing different types of people about the benefits of a risk management process will assist in revealing underlying risk attitudes, enabling systemic bias to be exposed and corrected.