IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4296

Quantitative Risk Assessment and the Effective Management of Software Projects

Dan Shoemaker[1], Antonio Drommi[2] and Wendy Norfleet[3]
University of Detroit Mercy, Michigan, [1]Tel: (313) 993-1170, [2]Tel: (313) 993-3337, [3]Tel: (313) 993-3338
[1,2,3]Fax: (313) 993-1673, {shoemadp, drommia, norfleew}@udmercy.edu

INTRODUCTION: THE PENALTY FOR NOT LOOKING BEFORE YOU LEAP

The essence of successful software management lies in the ability to gauge risks and evaluate performance. Or in simple terms, commitments should never be made where the likelihood of failure is prohibitive and/or project execution can't be tracked (Humphrey, 1994). The problem is that it is practically impossible to assess the risks of any prospective software project where there is either no prior experience, or the requirements are highly complex. And, as such, it is equally infeasible to expect to subsequently follow the process to its implementation.

As a result software busts schedules and budgets in a way that would not be tolerated in any other industry. It is a fact that…. *Depending on project size, between 25% and 50% of all projects fail, where "failure" means that the project is canceled or grossly exceeds its schedule estimates* (Laker, 1998). A recent Standish Group survey of 8,000 software projects found that the average exceeded its planned budget by 90 percent and its schedule by 120 percent (Construx, 1998). Several industry studies have reported that fewer than half of the software projects initiated in this country finish within their allotted schedules and budgets (Construx, 1998). This is not a new phenomenon. A study done by the GAO in the 1980s found that fully two-thirds of the software delivered to the federal government was never used and an additional 29% was never delivered at all. The good news was that 3% was usable after changes and 2% could be used as delivered. As a result, the GAO estimated that throughout the 1980s the federal Government's bill for worthless software topped $150 billion (Quoted in Humphrey, 1994). When 95% of the software delivered to the federal government is worthless you might expect some accountability. Yet numerous studies since then have identified the same problems. These include: *1) Poor project planning, 2) Inadequate documentation of project requirements, 3) Insufficient understanding of the business, 4) Lack of support and involvement from senior management, and 5) No written quality plan or no effective implementation of the plan* (SEI, 1997).

The Standish Group found that the most common causes of project failure were management-based considerations. That covered such things as incomplete requirements, lack of user involvement, lack of resources, unrealistic expectations, lack of executive support, and changing requirements. Those causes occurred with approximately equal frequency (Construx, 1998A similar study conducted by KPMG Pete Marwick found that 87% of failed projects exceeded their initial schedule estimates by 30% or more. While at the same time 56% exceeded their budget estimates by 30% or more and 45% failed to produce expected benefits. This resulted primarily from the following causes (KPMG, 1997)

1. Project objectives not fully specified (51%)
2. Bad planning and estimating (48%)
3. Technology that is new to the organization (45%)
4. Inadequate, or no project management methodology (42%)
5. Insufficient experienced staff on the team (42%)
6. Poor performance by suppliers of hardware/software (42%)

It would be a cop out to suggest that these failures were a consequence of extreme project size, or complexity. In actuality 60% of these failed projects were categorized by KPMG as small. The fact is that small projects (e.g., those that are characteristic of the average mom-and-pop software shop) are almost always over schedule (92%). In fact the larger, more complex projects actually did better. KPMG found that only 86% of these had problems meeting their delivery dates (which is still a pathetic statistic). One reason cited for the success of the big projects was that *formal project and risk management techniques were almost always employed in their management.*

Which leads to the inescapable conclusion that any organization, large or small, simple or complicated, functions better with some sort of defined process that will insure that the organization's people equipment and financial resources are utilized efficiently. This requires understanding all of the purposes and intents of the business. The most telling result of the KPMG study was the impact of the general business environment on software project success. Between 44% and 48% of the reasons for project failure came as a consequence of the failure of the software people to clearly understand how the business operated. Where projects failed the most common cause was a lack of project management (execution) and an inability to monitor project activity on the part of the project manager (KPMG, 1998).

That is why the quantitative management aims of level four CMM are so attractive to software managers. Those KPAs allow them to use the systematic data provided by the processes installed at that level and the prior two to evaluate potential commitments and monitor performance as the project unfolds. This in turn helps managers to identify and overcome the inevitable problems as they occur and minimize the risks of project failure.

Nevertheless, the problem with Level Four is that the prior two levels force the organization to change the way it does business. In fact, one of the primary stumbling blocks to the implementation of any externally imposed process improvement framework (be it CMM or ISO 9000) is that the company must adjust its current (and sometimes highly valued) structure and processes to meet the requirements of the model. While the methodology we are about to discuss achieves the same purposes as Level Four CMM (which is to improve organizational performance and increase productivity using focused management data) it is always developed internally. Consequently managers are supported in their efforts to evolve organizational functioning within the unique culture and norms of the business itself. Rather than forced to follow a staged, lockstep implementation scheme that can require considerable behavior change and generate unproductive resistance from among members of their own staff.

ASSESSMENT BASED RISK ESTIMATION: A SHORTCUT TO LEVEL FOUR

The methodology we are about to describe is based in principle on the assessment of the capability of a given set of defined processes. It provides information about the effectiveness of each of these processes in meeting business goals, whether those have been set for a

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

project, or the organization as a whole. The primary difference between this model and the way CMM Level Four defines capability is that it assesses each of these processes directly (based on a set of management attributes similar to the common features of CMM) to find out how capable it is, rather than depending on the yes/no presence of an installed processes to signify that. Thus it does not impose an organizational change solution. Instead it simply provides specific information about the effectiveness of each of the target processes, which managers can then use to evolve the organization to a higher level of productivity and efficiency. The key feature is that this information is obtained in a non-invasive way (e.g., one that is acceptable to the organizational culture as a whole).

The basis of this approach lies in the assessment of the level of adherence to commonly understood best practice. Over the past several years it has become manifestly clear that the only reference on which to base such an assessment are the lifecycle process definitions contained in the ISO 12207 (or if you prefer IEEE 12207.0) international standard (the best evidence of that might be the mass harmonization of the IEEE Standards Set to 12207 starting in 1995; Moore, 1998). The complete set of templates derived from this framework constitutes a fully defined software organization. Thus any roadmap assessment conducted based on such templates provides a picture of current status as well as a capability profile that can be used as a direct recommendation for achieving a fully defined and continuously improving software process. Functionally this assumes that a correct organization is one that performs the proper (to its purpose) primary processes along with all of the necessary supporting and organizational processes (as defined by 12207) independent of intricate phasing (as is the case with CMM). This means that information derived from such an assessment can help managers to both prioritize and plan for improvements in the functioning of each process based on the realities and constraints of their business situation (Gundry, 2001).

THE THREE-PASE RISK ASSESSMENT IMPLIMENTATION MODEL

The suggested way of implementing such a solution is in three organic phases. In the first (foundational) phase a standard based methodology is established and popularized within the organization. This involves selecting an appropriate standards set and the attendant methodologies. It does not involve forcing anybody to follow them. It merely entails a design function. Essentially the organization undertakes a process of deciding which coherent set of standards best fits its situation and philosophy.

The next phase begins, once a foundational set of best practices has been defined and agreed on. In this "Structural" phase a formal process is employed to install quantifiable, repeatable base practices and work products and the measures to assess them. Project launches and workshops are the means used to let the project manager establish a measurable and controllable project. The reader should note that this is an educational rather than a behavior change activity. The procedures and measures are introduced to the workforce as a whole through training, in-house consulting (conducted by designated champions) and mentoring not by requiring compliance to a procedure as a condition of performance. The output of the assessments provides executive management with performance ratings that let them judge how adequately base practices are being performed. In addition, it is this "adequacy" rating that allow them to assess the prospective and ongoing risks associated with the execution of the project.

In the third phase, the organization builds enterprise project management architecture. People in the organization who do not want to adopt this model are not forced to, but they are assessed using the foundational scheme as the index. Thus every project is monitored and continually assessed throughout the four phases of management – **Initiation, Planning, Execution and Closure**. Base practices and work products are employed as inputs to the assessment and (for ease of application) they are organized by a set of project types. Using the reference framework (built on the base practices of the ISO 15504 standard) it is possible to define 96 standard project types (for instance, *Supply – COTS*). These are all (by definition) modified through contract, contain base practices and work products specific to them, and are in a given phase of execution. The assessment creates a risk measure for the entire portfolio as well as for each individual project, thus providing all the information necessary to allow decision makers to formulate judgments about their execution. Any project, can be evaluated at any point in its functioning using this integration model. As a result, it is possible to determine the level of risk associated with a project at any point in its lifecycle. This amounts to the ability to describe in quantitative terms the project's capacity to be successful. In addition the risk associated with any project can be identified, mitigated and controlled. The total project risk is determined using the following inputs:

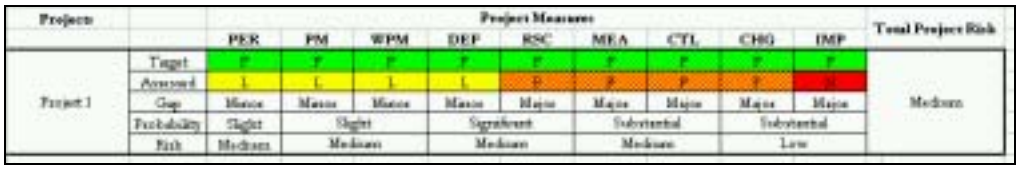
1. The expected, or target, rating for the project
2. The actual assessed rating for the project (e.g., Fully, Largely, Partly, Not)
3. The gap between the target and actual ratings (as a percent)
4. The probability for problems occurring because of that gap (as a percentage)
5. The risk of potential impacts from problems occurring (from the base practices guide)

Given the requirement for continuous systematic assessment within this model the explicit elements of data to support the risk assessment process must be defined. The following specific indices are used in the current process to support the assignment of potential risk *(n.b., for the portfolio and each project):*

- **Performance (PER)** – Extent to which base practices and work products are followed
- **Performance Management (PM)–** Extent to which the base practices are managed
- **Work Product Management (WPM)–** Extent to which work products are managed
- **Process Definition (DEF)–** the extent to which a process is defined for each project
- **Resource (RSC)–** Extent each project is resourced based on process requirements
- **Measurement (MEA)–** Extent to which the project is measured
- **Control (CTL)–** Extent to which the defined process is controlled by rational process
- **Change (CHG)–** Extent to which the process or product is changed by rational process
- **Improvement (IMP)–** Extent to which explicit continuous improvement actions exist
- **CSF** – other factors that are critical to the success of the project and must be present*(as defined by initial tailoring of the assessment process to the specific project)*
- **EAC** – the (currently) estimated budget required to complete the project
- **CPI** – is the project projected to be over or under budget?
- **SPI** – is the project ahead or behind schedule?
- **Time to market** – Projected timeframe to achieve ideal project management goals
- **CV** – Dollar amount the project is over or under budget?
- **Defects** – is the defect rate rising or falling?
- **Defect locations** – what is the number of defects and cost of repair per project element?
- **Changes** – average number of requested changes per project?
- **Change locations** – where do changes occur and how much do they cost to implement?

Building upon the foundational and structural PMO This is captured and presented in a Project Risk Analysis Report. The following example represents an analysis of three different projects. The first (*figure one*) is a medium risk effort. The second (*figure two*) is a low risk undertaking and the third is high risk. The colors represent the rating of the management attributes characteristic of successfully per-

Figure 1: A medium-risk project

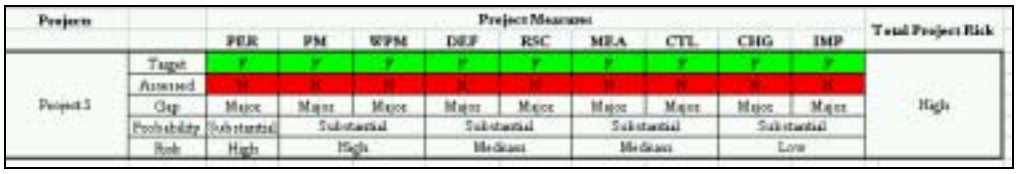


Projects		Project Measures									Total Project Risk
		PER	PM	WPM	DEF	RSC	MEA	CTL	CHG	IMP	
Project 1	Target	F	F	F	F	F	F	F	F	F	Medium
	Assessed	L	L	L	L	P	P	P	P	N	
	Gap	Minor	Minor	Minor	Minor	Major	Major	Major	Major	Major	
	Probability	Slight	Slight		Significant		Substantial		Substantial		
	Risk	Medium	Medium		Medium		Medium		Low		

Figure 2: A low-risk project

Projects		Project Measures									Total Project Risk
		PER	PM	WPM	DEF	RSC	MEA	CTL	CHG	IMP	
Project 2	Target	F	F	F	F	F	F	F	F	F	Low
	Assessed	F	F	F	F	L	L	P	P	P	
	Gap	None	None	None	None	Minor	Minor	Major	Major	Major	
	Probability	None	None		Slight		Significant		Substantial		
	Risk	None	None		Low		Low		Low		

Figure 3: A high-risk project



Projects		Project Measures									Total Project Risk
		PER	PM	WPM	DEF	RSC	MEA	CTL	CHG	IMP	
Project 3	Target	F	F	F	F	F	F	F	F	F	High
	Assessed	N	N	N	N	N	N	N	N	N	
	Gap	Major	Major	Major	Major	Major	Major	Major	Major	Major	
	Probability	Substantial	Substantial		Substantial		Substantial		Substantial		
	Risk	High	High		Medium		Medium		Low		

forming the activities represented by the first nine indices. The potential levels of performance are (F) Fully, (L) Largely, (P) Partly and (N) Not. For instance, the first cell in the first project states that the base practices (PER) are (assessed as) (L) Largely fulfilled whereas the target is (F) Fully. Which produces a minor gap and a slight probability of failure. Thus the risk associated with that would be medium.

Given that the intent of process assessment is to identify the risk associated with the delivery of a product, the other dimension is the capability domain. Alternatively, in simple terms the project's process capability describes risk. Because the assessment model is based on the ISO 15504.CMMI classifications, capability is defined on a six-point ordinal scale (levels 0-5). The scale represents increasing capability

Table 1: Process attribute ratings

PROCESS ATTRIBUTE RATINGS		
Fully Achieved	**86-100%**	**F**
Largely Achieved	**51-85%**	**L**
Partially Achieved	**16-50%**	**P**
Not Achieved	**0-15%**	**N**

from performance that is not capable of achieving its goals (level 0: Incomplete), to performance that is capable of meeting relevant process and improvement goals that are explicitly derived from the organization's business plan (level 5: Optimizing). The measure of capability is based upon a set of attributes - each of which measures a particular aspect of the process capability. The attributes themselves are measured on a percentage scale and therefore provide a more detailed insight into the specific aspects of a project. This scale is shown below:

A target capability profile is used to judge process capability. This profile is based on pre-defined project types, the required process attributes of each project type and the achievement rating deemed necessary for each attribute. The target profile represents the minimal acceptable process-oriented risk. It should be noted that risk arises from inappropriate process management - i.e., not deploying appropriate management practices, or from deploying them in a way that is does not achieve the required goals. Process attribute gaps are calculated by comparing the target capability profile to the assessed capability. Because it would not make sense to seek to achieve a low level of capability the target capability profile consists only of Largely Achieved and Fully Achieved target ratings. The process attribute gaps and the subsequent impact ratings are shown in Table 2.

The extent of the identified gap then determines the probability of problems occurring within a capability level, as described in Table 3:

Therefore, when the capability level in which the gap occurs is cross-referenced against the extent of the gap, the level risk can be characterized, as show in Table 4.

Finally, besides risk assessment (which doesn't resonate too

Table 2

TARGET RATING	ASSESSED RATING	GAP
Fully Achieved	Fully Achieved	None
	Largely Achieved	Minor
	Partially Achieved	Major
	Not Achieved	Major
Largely Achieved	Fully Achieved	None
	Largely Achieved	None
	Partially Achieved	Major
	Not Achieved	Major

Table 3

NUMBER OF PROCESS ATTRIBUTE GAPS WITHIN CAPABILITY LEVEL	PROBABILITY
No major or minor gaps	None
Minor gaps only	Slight
A single major gap at Level 2-5	Significant
A single major gap at Level 1, or more than one major gap at Levels 2-5	Substantial

Table 4

LOCATION OF GAP	PROBABILITY			
	NONE	SLIGHT	SIGNIFICANT	SUBSTANTIAL
Optimizing (Level 5)	None	Low	Low	Low
Predictable (Level 4)	None	Low	Low	Medium
Established (Level 3)	None	Low	Medium	Medium
Managed (Level 2)	None	Medium	Medium	High
Performed (Level 1)	None	Medium	High	High

well with the average CEO) it is also possible to generate quantitative cost estimate (which does). This is the final and most valuable (to decision-makers) benefit of assessment using this model.

CONCLUSION

As can be seen, any software project, large or small, simple or complex, can be assessed using this approach. That amounts to the ability to quantify each supplier's capacity to successfully deliver the project. The risk associated with selecting a certain supplier can then be translated into an objective index, which the acquirer can account for and control. The Risk Assumed scale enumerates the ***management*** capability of the project, which is measured based on the management practices that are embodied in the assessment. You should (finally) note that the risks identified are at the overall organizational management level and they should be considered separate from software engineering risks that are identified and mitigated during the project life cycle. Furthermore, one way to distinguish management risk from typical project execution risks might be that the risk rating captures the supplier's ability to manage risks during the project life cycle. Thus the information derived from this model can objectively identify which projects are at risk ***before*** the project starts. This enables an organization to focus on and manage the risks identified as most likely to cause the project to fail during its lifecycle. That in its self is immeasurably valuable.

REFERENCES

1. Boehm B., Improving Software Productivity, Computer, Volume 20, Number 9 September 1987
2. Card, D. and E. Comer, *Why Do So Many Reuse Programs Fail?,* IEEE Software, September 1994
3. Construx Software Builders, web site @ www.construx.com, accessed, August 2001
4. Curtis W., *Building a Cost-Benefit Case for SPI*, 7th SEPG Conference, Boston, 1995
5. Dion, R., *Process Improvement and the Corporate Balance Sheet*, IEEE Software, July 1993
6. Dorofee A.J., JA Walker, RC Williams, Risk Management in Practice, Crosstalk, Volume 10 #4, April 1997
7. *Evaluating Information Technology Investments*, Office of Management and Budget, at www.itmweb.com, accessed August 2001
8. Fenton N, *How Effective are Software Engineering Methods*, Journal of Systems and Software, Volume 22, 1993
9. Gundry, Edward and Dan Shoemaker, Requirements Based Estimation", Decision Sciences International Conference, Proceedings, San Francisco 2001
10. Humphrey, Watts,, *A Discipline for Software Engineering*, Addison-Wesley: Reading, MA, 1995
11. Humphrey Watts S., *Managing the Software Process*, Addison-Wesley: Reading, MA, 1994
12. International Organization For Standards, *ISO/IEC 12207*, Geneva Switzerland, 1995
13. International Organization for Standards*, TR- 15504*, Geneva, 1998
14. KPMG Technology and Services Group, web site at www.kpmg.ca accessed September 2001
15. Laker Consulting, web site at www.laker.com.au., Sydney, accessed August 2000
16. Lee, E. *Software Inspections: How to Diagnose Problems and Improve the Odds of Organizational Acceptance,* Crosstalk, Vol.10 #8 1997
17. McGarry F. and K. Jeletic, *Process Improvement as an Investment: Measuring its Worth*, NASA Goddard Space Flight Center, SEL-93-003, 1993
18. McGibbon, Thomas, *A Business Case for Software Process Improvement Revised*, DoD Data Analysis Center for Software (DACS), 1999
19. Rozum, J., *Concepts on Measuring the Benefits of Software Process Improvement*, CMU/SEI-93-TR-09, ESC-93-TR-186, June 1993
20. Software Engineering Institute, web site at www.sei.cmu.edu. Accessed 1998
21. Strassman, P.A., The Business Value of Computers, The Information Economics Press, New Canaan, Connecticut, 1990