Assessing Software Risk

Louis A. Poulin
GRafP Technologies Inc.

This article describes the application of hazard evaluation and prevention to software risk management. This approach has been used by organizations involved in developing information technology (IT) applications in order to assess the probability that serious problems will occur, such as cost overruns, schedule slippage, and products or services that do not satisfy their intended needs.

Prevent Losses, Maximize Opportunities

Most risks arise from dealing with change. Any change translates into a loss or an opportunity, each requiring a decision that in turn will generate more changes, as shown in Figure 1. This can lead to an avalanche effect (usually destructive), or it can be channeled to have a constructive outcome.

In any situation at least three main axes should be considered when attempting to prevent losses for a given entity: the human resources associated with this entity; the tools, equipment, and technology used in (or by) this entity; and the mission that this entity is pursuing (or the function it is performing). Assume that five changes can occur along each axis over a given period of time. Each change offers either a loss or an opportunity. If there are two ways to prevent the loss from occurring and two ways to take advantage of the opportunity, any one change requires examining a total of $C^{2}_{90} = 4,005$ relationships before making an optimal decision. Given that at times several changes may occur over a period of one day, this is not an easy task, as depicted in Figure 2, which includes only one change per axis. Napoleon Bonaparte's statement to the effect that all he wanted from his generals was that they be lucky, is therefore not entirely surprising.

Obviously problems that have been anticipated are more likely preventable. Just implementing a few preventive measures perfectly matched to an undesirable event increases the likelihood of preventing losses. Conversely, even a large number of preventive actions are liable to be ineffective if potential problems are poorly anticipated. Crises are bound to occur sooner or later.

For example in the Vietnam conflict, the North Vietnamese were definitely more successful than the French and the United States even though they did not have access to all the material resources that the latter had. Yet they demonstrated great ingenuity at exploiting what they had at their disposal to address the challenges they were facing. It is indeed remarkable that they were able to hold out for so long against two world powers.

It should nevertheless be possible to devise a set of *mechanisms* to monitor undesirable conditions and to prevent problems from occurring. In this way, it becomes possible for an entity to operate at an arbitrarily low likelihood of losses as long as it has the capacity to implement such mechanisms [1].

Application in Software Engineering

Among the fields where the aforementioned principles have been put into practice, assessing risk in IT projects [2] is the one in which we have collected the most information. In these assessments three basic parameters were measured: the risk perception level, the risk mitigation capacity, and the likelihood of problems.

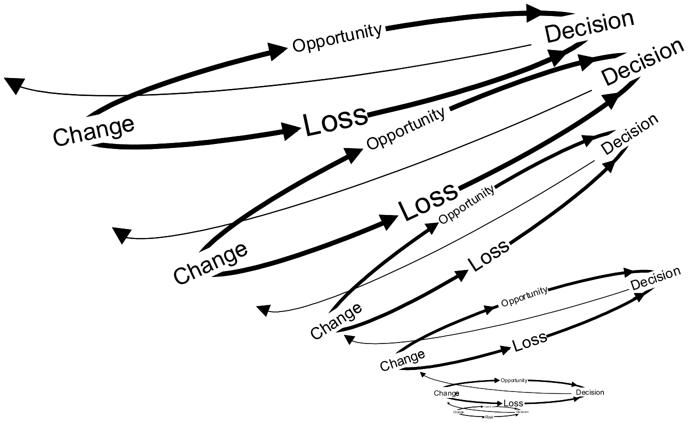


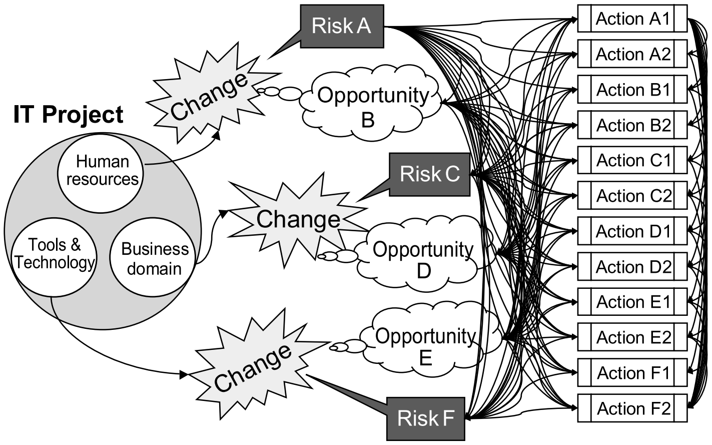
Figure 1. *Loss vs. opportunity*

The Software Engineering Institute's Capability Maturity Model® (Levels 2 and 3) and the Taxonomy-Based Risk Identification [3] were used as the IT assessment framework.

The risk perception level corresponds to the ability to anticipate problems. In an IT context, it is the capacity of professionals assigned to a project to anticipate potential problems and take preventive actions. To some extent, this capacity depends on personnel experience and know-how. It also depends on the risk mitigation capacity because a mature process has a greater capacity to anticipate problems through information provided by its risk mitigation components. In fact, such a process may compensate for a lack of experienced personnel.

In other words, an organization may decide to hire very talented and experienced, high-salaried people to develop the IT application with the help of a minimal and less expensive process. Or it can decide to implement an expensive high-maturity process and hire less experienced, less expensive people. A cost-effective compromise may be to hire a few talented and

Figure 2. *The complexity of preventing losses and exploiting opportunities*



experienced people to develop and implement a high maturity process that captures their know-how and experience, which less experienced people can subsequently apply.

The risk mitigation capacity corresponds to the mechanisms in place to prevent problems. In this context, risk mitigation capacity is similar to process capability, taking into account that some process components have more risk mitigation potential than others.

Finally, the likelihood of problems is the probability that risks will materialize. Again, given the IT framework and defined assessment scope, this represents the probability that serious problems will occur jeopardizing the project or causing failure. Risks in this case include cost overruns, schedule slippages, and products or services that do not satisfy their intended needs.

The experience gained in the course of conducting such assessments has shown that in IT, risks are basically divided into two classes: process-related (common or frequently recurring) risks and project-specific (singular or infrequently recurring) risks. Process-related risks originate from the way methods, tools, procedures, and human resources are integrated to produce a desired outcome. Their nature makes them more prone to recur from project to project (e.g., conditions leading to critical decisions being unduly delayed or taken without having access to all relevant information). Project-specific risks are intimately linked to the nature of a project and are therefore less prone to recur (e.g., conditions leading to a system being unable to handle the volume of information it must process because of network bandwidth limitations).

The breakdown of problems encountered in organizations having undertaken IT projects, based on the information collected so far, is shown in Table 1. This data indicates that process-related risks account for 70 percent of all risks in IT projects where risks of unknown nature are distributed along the ratio of process-related to project-specific risks. In fact, a more accurate statement would be that, on average, risks in IT projects are made up of 30 percent project-specific components and 70 percent process-related components.

Risk Assessment Results Summary

The data collected so far in Europe, South America, and North America using this approach indicates that an IT project has a 33 percent probability of experiencing serious difficulties, including cost overruns, schedule slippage, and products that do not generate anticipated benefits. In terms of frequency, 33 percent of IT projects can expect to experience such problems to the point of failure. This also confirms the finding documented by the Standish Group International showing 31 percent of IT projects are cancelled before completion [4].

Assessment data also showed that, at least in IT, the critical threshold associated with the likelihood of problems appears to be approximately 40 percent. In other words, a project or an organization cannot sustain a likelihood of problems higher than 40 percent for any significant duration relative to the planned or current activities. Consider that a likelihood of problems equal to 50 percent corresponds to operating at random. If such were the case, it would be wishful thinking to expect any successful outcome over a significant period of time.

Source of Observed Problem (a risk that materialized)	Nature	Relative Freq. of Occurrence
Customers (e.g. poor communication of requirements)	Mostly process-related	15%
System components (e.g. inadequate technical performance)	Mostly project-specific	14%
Development methods (e.g. improper design approach)	Mostly process-related	13%
Management (e.g. critical decision unduly delayed)	Mostly process-related	12%
Suppliers (e.g. inability to deliver as planned)	Mostly process-related	12%
Change management (e.g. incompatible components)	Mostly process-related	10%
Development environment (e.g. unsuitable programming language)	Mostly project-specific	9%
Tests (e.g. incomplete test coverage)	Mostly project-specific	6%
Supervision mechanisms (e.g. irregular tracking of progress)	Mostly process-related	5%
Others	Unknown	4%

Table 1. *Breakdown of problems in IT projects*

The same 40 percent value holds true in the financial industry (venture capital), where a portfolio manager will tolerate four investments out of 10 not generating a profit [5]. Anything higher than this ratio will result in restructuring the portfolio in order not to exceed the 40 percent limit, which would result in a certain loss.

The assessment approach has also been used to characterize the Canadian IT industry. Data was collected through 30 comprehensive assessments conducted in Canadian organizations involved in developing products or providing services drawing on IT and software engineering. The size of the assessed organizations ranged from 10 professionals to 250, with an average of 76, and a standard deviation of 64. Table 2 summarizes assessment results.

The results indicate that with a likelihood of problems at 34.3 percent, Canadian organizations can expect to face slightly more difficulties than the average organization, which is characterized by a 33 percent value. Out of the 30 assessed organizations, eight exceeded the aforementioned 40 percent threshold, and in all cases, major difficulties were observed during the 12 to 18 months that followed.

Government organizations have a higher risk mitigation capacity than private industry. But the latter has a higher capac-

Table 2. *Assessment results for all assessed government/private organizations*

	All Organizations		Government Organizations		Private Industry	
Parameter	Average	Standard deviation	Average	Standard deviation	Average	Standard deviation
Risk Mitigation Capacity	60.1%	9.1%	62.9%	11.0%	57.9%	6.9%
Risk Perception Level	38.0%	9.4%	34.0%	10.7%	41.0%	7.2%
Likelihood of Problems	34.3%	11.0%	34.3%	10.9%	34.2%	11.3%

ity of anticipating problems and taking appropriate action. The end result is that both are characterized by the same likelihood of experiencing problems (34.3 percent vs. 34.2 percent).

Reliability of the Approach

A trial was conducted in 1999 with a large government IT project to determine the reliability of the approach. The project called on new technologies and a large pool of resources that did not necessarily share the same processes. It also had particularly challenging coordination aspects stemming from the wide geographical distribution of stakeholders.

On a general level, the trial's main objective was to determine the level of correlation between intrusive (or active) risk assessment techniques such as taking a subsystem apart, conducting audits and inspections vs. non-intrusive (or passive) risk assessment techniques (e.g. keeping a subsystem under remote surveillance or conducting collaborative appraisals). A second objective was to assess the degree of correlation between the measured likelihood of problems when 259 process-embedded risk mitigation mechanisms were investigated versus 404. The number of undesirable situations that are most often encountered in the course of developing or maintaining IT applications was fixed at 163 in both cases. Table 3 summarizes the results of the trial.

The correlation between non-intrusive and intrusive assessment techniques was not as high as expected. In fact, non-intrusive assessments were found to be more accurate than intrusive assessments after the data analysis was completed; intrusive assessments do have an impact on the likelihood of problems because of their disruptive effect on the collected information. On the other hand, non-intrusive assessments do not seem to be overly affected by noise, a concern that had been expressed regarding the use of such techniques. Non-intrusive assessments exhibited a surprisingly high level of correlation considering that two independent teams conducted the field trial. However, while relatively immune from noise, non-intrusive assessment techniques alone tend to be pessimistically biased, whereas intrusive assessment techniques tend to be optimistically biased. Non-intrusive assessments followed by intrusive assessments seem to provide the best results. In this case for an investigation of 404 mitigating mechanisms, the results were: a likelihood of problems of 33.7 percent, a risk mitigation capacity of 61.2 percent, and a risk perception level of 36.7 percent.

Conclusion

The importance of assessing software risks and of subsequently managing them has slowly been gaining recognition over the last decade. Common sense indeed dictates that reducing the frequency of problems in the course of an IT project will increase the likelihood of a successful delivery.

Through assessments we have conducted during the years, we have observed that the most successful organizations are those that have established sound processes for carrying out their projects while concurrently focusing on anticipating problems and preventing them from occurring. Individuals are known to operate at a constant risk level, and as problems are better anticipated and dealt with, larger projects that present a higher level of risk are initiated, which in turn contribute to the growth of the organization.

	Non-Intrusive Techniques 404 Mitigating Mechanisms	Intrusive Techniques 404 Mitigating Mechanisms	Non-Intrusive Techniques 259 Mitigating Mechanisms
Likelihood of Problems	37.5%	31.0%	37.8%
Risk Mitigation Capacity	58.6%	63.0%	58.0%
Risk Perception Level	36.7%	36.7%	37.3%

Table 3. *Summary of field trial results*

It is worth quoting Andrew Grove, CEO of Intel Corp., a company that has had a major impact on IT, in his book *Only the Paranoid Survive.* According to Grove, "Sooner or later, something fundamental will change in your business." The Wallace Corp. is a good example; it won the prestigious Malcom Baldridge Award in 1990 and declared bankruptcy in 1991.◆

References

1. Gallager, Robert G., *Information Theory and Reliable Communication*, John Wiley and Sons, New York, 1968.
2. Poulin, L.A. and Michael Raftus, *Software: Process Risks Identification, Mapping and Evaluation,* Proceedings of the SEI Conference on Risk Management, Virginia Beach, Va., April 1997.
3. Dorofee, Audrey J., Higuera, Ronald P. et al., *Continuous Risk Management Guidebook,* Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Pa. 1996.
4. *Chaos—Application Project and Failure,* The Standish Group International, January 1995.
5. Worzel, Richard, *From Employee to Entrepreneur,* Key Porter Books, Toronto, 1989.

About the Author

Louis A. Poulin assesses the capability of IT organizations and develops hazard evaluation, monitoring, and prevention tools and methodologies. He has a bachelor's in engineering physics, a certificate in Naval engineering, and a master's in electrical engineering. He supervised the development of the tool used to carry out the assessments described in this paper. Previously, Poulin served in the Canadian Navy as a Combat Systems Engineering Officer. He is a member of the Institute of Electrical and Electronics Engineers and a fellow of the Engineering Institute of Canada.

GRafP Technologies Inc.
550 Sherbrooke St. West, Suite 777
Montreal, Canada, H3A 1B9
Voice: 514-847-0900
Fax: 514-847-0400
E-mail: lpoulin@grafp.com
Internet: www.grafp.com