

Essential Risk Management

Robert N. Charette, ITABHI Corporation

This paper is an outgrowth of personal experience gained in conducting risk analysis and management on various types of information systems, from real-time to MIS, over the past 15 years. Over this period, I have performed a wide range of risk management tasks associated with computing systems. These range from aiding project managers in charge of small software engineering projects trying to understand the technical risks a new bit of information technology created, to corporate controllers of multi-billion dollar companies who were trying to understand the business risks to their corporation of implementing hundred million dollar infrastructure information systems.

What I have discovered is that while risk management is applied in some form throughout most organizations, its purpose and relationship with other management/technical disciplines are fundamentally misunderstood by managers at all levels of the organizational spectrum. This incorrect perception typically creates several common pitfalls and problems in its application, often to both the near and long term detriment of the organization.

In this paper, I will relate some of my experiences, especially those concerning the difficulties organizations have in separating risk from problem management. I will attempt to explain why this occurs and postulate a means via a general risk framework model to help overcome this situation. I believe that clarifying this issue is critical if risk management is not to

become yet another fad in the software engineering community that is oversold.

Risk vs. Problem Management

From my experience, the single greatest obstacle people have with the concept of risk management is in distinguishing it from that of problem management. The two are so closely intertwined that risk management is often perceived as problem management, and therefore is of no special consequence. This perception makes not only the “selling” of the importance of risk management difficult, but makes its correct application an uphill battle as well.

The confusion is easy to understand, since: (1) people practice problem management every day, whereas risk management is not; (2) people have been trained to think about resolving problems, or exploiting opportunities, but not risks; (3) risk is an unpleasant, emotive word that often makes the subject taboo in organizations; (4) problem management and risk management use the same underlying processes, which add to the confusion, and; (5) problem management is intuitive, whereas people are uncomfortable dealing with the “technical” aspects involved in risk management such as probability. Further adding to the difficulties is the fact that in some situations, say in trying to deal with the effects of a crisis, problem management is risk management.

To untangle the web a little bit, we need to understand that problem management is in actuality a proper subset of risk management. This implies that everything that is done to manage a problem (e.g., the process and techniques used) also exists in risk management, but not necessarily conversely. In fact, problem management equals risk management when you

“do not look past today,” as it were. As we will see later, time is an important characteristic that we will use to distinguish between the two.

Second, problem management is usually being performed on past risks that have come into existence. This causes difficulty in trying to define where risk management ends and problem management begins. In our practice, I attempt to overcome this difficulty by telling our clients that risk management concerns the potential future effects of current decisions, while problem management deals with the current effects of past decisions. In other words, as I have depicted in Figure 1, past becomes prologue, as yesterday's risks are today's problems, whereas some of today's risks may be tomorrow's problems.

Third, organizations are performing risk management as part of their problem management process, even if they do not quite realize it. For example, a project manager will speak of future or potential problems, i.e., risks, and the action he needs to take to deal with them. It is very unusual,



Figure 1. Past is Prologue

however, for a project manager to verbalize that he or she shall apply risk management to potential problems, but problem management to current ones. The distinction just does not exist yet in the project manager's mind or vocabulary, yet it is vital that it does if risk management is to grow in importance.^{1,2,3}

I strive to get project managers to make this distinction by framing the difference in terms of resource utilization, i.e., in risk management, current resources are spent on future issues, while in problem management current resources are spent on current problems. This seems to help clarify the difference.

Fourth, when risk management is distinguished from problem management, the distinction is often bound to the use of some “risk management” technique. In other words, techniques, such as decision trees, risk lists, isorisk charts, Monte Carlo simulations, etc., are (mis)taken as characterizing the risk management process.⁴ This is similar to what occurred in the early

¹ Words freeze ideas. If the concept of risk management cannot be separated from that of problem management then it will never flourish.

² As will be explained shortly, the result of problem management is a solution which itself possesses a risk. These risks may or may not occur and may be the cause of more problem management themselves. Risk management tries to eliminate the root causes of risk wherever possible, but frequently, only their impacts can be reduced.

³ Where one finds risk management specifically separated from problem management is in organizational specialist groups, such as strategic planning, where the future *is* their business. However, one finds little link between this activity and the day-to-day problem solving that takes place within IS projects. Some specific risk management activity is often found in initial project planning, or in bid management, but once the plans are adopted and placed into execution, problem management tends to dominate.

By using risk management as part of the planning phase, however, it becomes “invisible.” In other words, if a risk is not encountered due to diligent risk management, then it will get little or no credit (it is hard to “prove” that risk management caused the risk to be avoided because you are trying to prove a negative—its like trying to prove that counter terrorism measures are effective). Similarly, if a risk does occur, say an act of terrorism when anti-terrorism measures are undertaken, than the risk management procedures are likely to get a lot of the blame. For a discussion of these and related issues, see “Risks of Risk Analysis,” Robert N. Charette, CACM, June 1991.

⁴ The Air Force, for example, has standardized on a tool called SEER/SEM to help determine the cost and schedule risks for systems involving software. The weakness to this approach,

days of quality, when quality control techniques such as inspections were viewed as representing or embodying the quality process, instead of the other way around. I try to overcome this point by using the aforementioned quality analogy, as well as by emphasizing process over technique, i.e., by defining a risk management process which techniques help to implement (similar to the software engineering model of process, methods to support the process, and where possible, automation of the methods).⁵

If you examine the symptoms of the confusion that exists between risk and problem management, you can begin to see that their root causes are created by three distinct elements: time, information and control. In fact, these three elements can be used to begin to characterize the differences between risk and problem management, as shown in Table 1. For example, as I have already pointed out, problem management is concerned with current issues, not (necessarily) future ones.⁶ Generally, the time horizon of the impacts or effects of conducting problem management is very limited, whereas risk management deals with an extended time horizon (risk management “shifts the time domain” as it were).

The informational and control horizons also differ between problem and risk management. When dealing with a problem, for instance, the informational boundary conditions are generally fixed (i.e., the problem exists), whereas risk management deals with boundaries that are fluid. The same generally holds true for the scope of control.

of course, is that the tool makes certain assumptions that may not be relevant and as with all tools, garbage in, garbage out.

⁵ See Charette, Robert N., *Software Engineering Environments: Concepts & Technology*, McGraw-Hill, 1986.

⁶ This is a sticky point to many people. The question we are usually asked is, “Well, doesn't problem management also impact the future?” which, of course, it does. The point is that the focus on problem management is on dealing with the current effects of yesterday's actions, not the effects of today's actions on tomorrow.

What is interesting but unsurprising is that the lack of time, control, and (or) information are also the root causes of risk. Problem management, by dealing with very short or narrow time, control and information horizons, can only deal with the symptoms of the specific and existing problem encountered. Contrast this to risk management that is aimed at trying to eliminate root causes of the specific problem as well as any future problems of a similar nature.⁷ This difference also helps explain why, when risk management is not undertaken by an organization, that today's problems often end up being more severe than necessary, and become usually repetitious in nature.

	Information Domain	Time Domain	Control Domain
Risks	Wide	Long	Loose
Problems	Narrow	Short	Tight

Table 1. Differences Between Risks and Problems

Finally, we try to get our clients to understand that risk management and problem management have complimentary, but different goals. The purpose of risk management is to attempt to eliminate the root causes of risk, i.e., future or potential problems, whereas the objective of problem management is to find a solution to a particular problem that is now existing. That solution may itself have some risks associated with it that need to be dealt with via risk management techniques. Sometimes the solution to a problem will eliminate the risks, but this is a side effect of the process, instead of its

⁷ One cannot eliminate risk per se, but only its root causes. The risk of fire, for example, is always a possibility, but we can eliminate it in a specific circumstance if we eliminate its potential causes. Thus, when we state that we are going to eliminate risk, it should be understood that we are trying to eliminate the root causes of risk.

primary goal (eliminating future problems while not solving the current ones would not be considered successful problem management).

Risk Management & Decision-Making

Although the characteristics of time, control, and information are helpful in distinguishing problem from risk management, we really need to step back yet again and discuss a basic property that they both have. Both the management of risks and the management of problems are essentially about the management of change, and the choices that change creates, as shown in Figure 2. A problem, after all, is the result of some decision taken (or not, as were the case).⁸ A risk, therefore, is just a hypothesis of a potential problem, which, if acted upon early enough, may be able to be avoided.⁹ By solving a problem, new risks and new choices are created.

It is our belief that through the **simultaneous** management of risks and problems involved in a decision that change itself is eventually managed, and future choices are enabled or removed.¹⁰

⁸ We note that if there are no choices, one does not have any risk: one only has certainty (i.e., a problem to solve).

⁹ Although we have not mentioned it explicitly, there is a precedence ordering between problem and risk management. Risk management takes place before problem management. This can be seen by considering again that a plan is nothing more than a postulated set of decisions that take place over the future. Since a plan is not yet reality, one will perform risk management first on these “virtual decisions” to eliminate risk. Once the plan is finished and is placed into execution, and then some change in the plan is required, problem management (and/or risk management) comes into play. Again, there is the vocabulary problem as typically people will refer to removing potential problems via the plan, which in their mind is problem management, but is in fact risk management. Thus, one can also characterize risk and problem management based upon when they are used, as well as how they are used.

¹⁰ Recall that while we are dealing today with the current effects of past decisions, we are faced with making new choices with new risks as a result of changing the situation through our problem solving actions. Furthermore, one needs to perform good problem management today *for there to be any tomorrow to worry about*.

Thus, risks and problems must concurrently be dealt with, but in either case, the way to deal with them is through decisions. We can therefore conclude that risks (and problems) are tied to the choices we make, and this means that the management of risk (as well as problem management) is inextricably tied into making decisions.¹¹

This concept is illustrated further in Figure 3, which depicts a simple, six-stage decision making process. As one can see, the very first step that starts

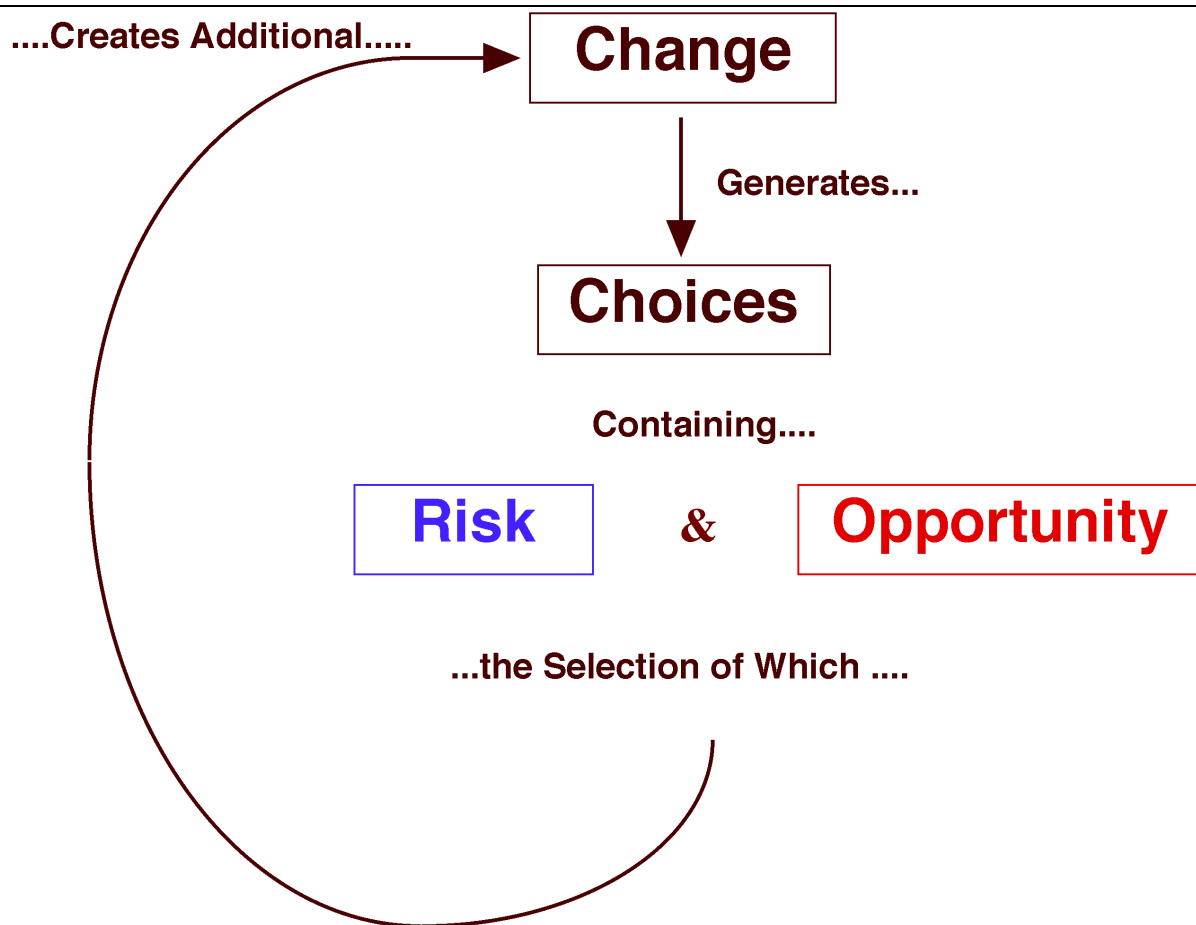


Figure 2. Risk Paradigm

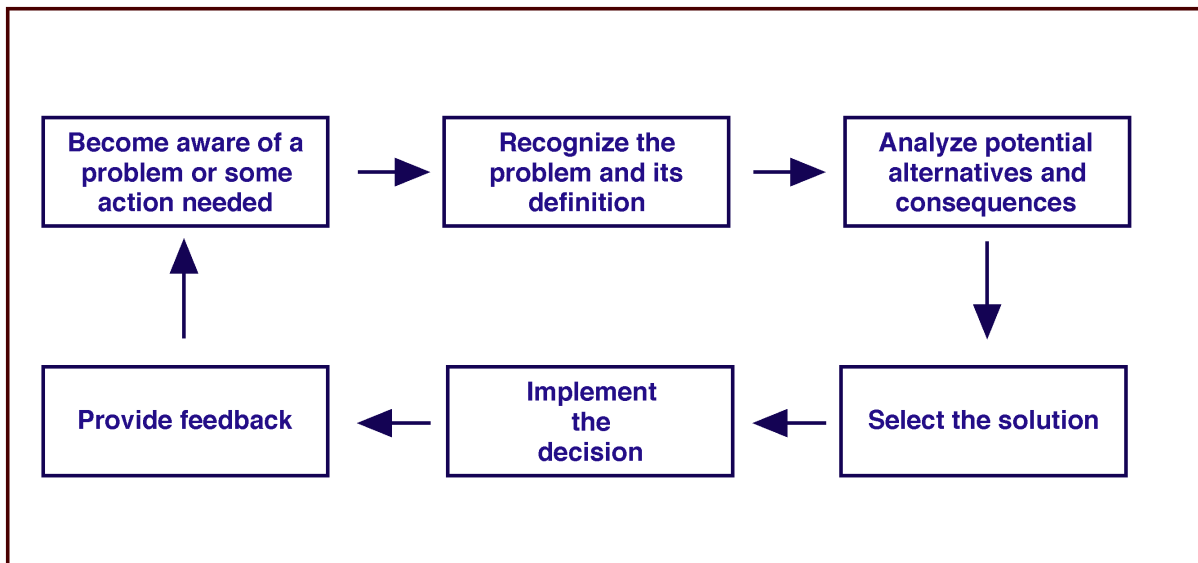
¹¹ This, of course, assumes a “rational” model of decision making within an organization. Nils Brunsson, in his book, *The Organization of Hypocrisy*, challenges the link between decision making and action within an organization. He tries to demonstrate that decision making is often used as a means to not act, or to avoid responsibility. These points and other, also influence why risk management is not taken seriously, and in many cases poses a

the process off is the awareness of some problem or action (i.e., decision) is required.¹² Some **change** to the current situation is needed. If there were never any change, there would not exist any need to make choices.

Notice in the diagram that I have drawn a box around the decision making process. This isn't a graphical device, but is the boundary around which we define the scope of change we plan to concern ourselves with (i.e., the horizons referred to earlier). When I spoke above about the differences between risk and problem management, what we really are discussing are differences in the degrees and magnitude of change that both deal with.

In our experience, defining the boundary creates many of the difficulties appearing in the risk management practice. If the boundary is drawn too tightly, then risk management again becomes just problem management.

Boundary



Boundary

Figure 3. Decision Making Process

threat to management. For further information, see Nils Brunsson, *The Organization of Hypocrisy*, John Wiley & Sons, 1989.

¹² The Japanese call this state *warusa-kagen*.

This produces a side effect of forcing the problem solver to ignore the temporal aspects of potential future problems (because of being overwhelmed by the “here and now”). This again almost guarantees that the problems that will be faced tomorrow will be more severe than they might have been.

I often see the decision boundary tighten because the decision-makers view that certain issues are beyond their scope of control, which is often true. Thus, even if risk management is performed, the overall benefit is reduced, as “outside the boundary” actions swamp any actions to eliminate risk. The result is that decision-makers become more reactive problem solvers. As will be discussed a bit later, for risk management to succeed, it must occur at each level within an organization so that the decision-making boundary is as wide as possible.

Boundary Conditions, IS & Organizational Maturity

You can see how the boundary definition is critical to risk management as it applies to information systems, for what is in the decision making process (i.e., the context or boundary) is dependent upon the maturity of an organization in its use of information systems. This can be observed in Figure 4, which depicts organizational information technology utilization over time.¹³ An organization travels through a number of learning stages in its use of information technology.¹⁴ As the organization matures in its use of IT, information technology touches more and more of the organization as the organization understands what information systems can do for (and to) its

¹³ Figure 4 is based upon an original graphic created by Nolan Norton, published in *Workstations and Networks*, 1989.

¹⁴ Each phase is an “S” shaped learning curve. Notice the overlap of each with the other, as well as the extended period required as more and more of the organization is covered. Part of the reason for the extended period is not only that more is being changed or impacted by IT application, but that all the previous application approaches to applying IT require re-examination to determine whether they can be made more effective, or better yet, redundant,

business operations. The impact of change also becomes greater and greater as information system utilization becomes more sophisticated.

What this means is that the boundary around the decision domain, i.e., the amount and impacts of change, will expand over time, as do the time, information, and control horizons that need to be dealt with. This has several important implications. The first is that at the beginning, within the elements of an organization where there is little relative change owed to introducing information systems, risk management and problem management will almost assuredly be identical in nature.

Re-examine Figure 4 and the area labeled automated tasks and individual learning. The scope of change of introducing information systems deals mainly with changes to procedures and tasks. These tasks are seldom used daily, but are more likely weekly or monthly tasks (payroll accounting, for example). Further, the boundary of the change introduced is along a technical boundary, e.g., what technology do we need to change to perform these tasks, as opposed to what business process we need to change. Matters of making current processes more efficient dominate the planning process. The time, control, and information boundaries are narrow, as are the ultimate effects of any changes made. The decision process illustrated in Figure 3 will be primarily focused on problems that deal with how information systems affect current procedures and tasks.

Yet, as the organization becomes more sophisticated, it begins to automate business processes. This action now rapidly increases the horizons to include issues that are not only technical in nature but also organizational. Intra-function and cross-function organizational elements are involved, making the effects of change greater, but also longer to see. Another way of stating it is

and thus eliminated. Thus, when doing a strategic business vision, the past tactical and technology driven visions have to be considered again as well.

that the environments of interest that we are dealing with have expanded greatly. Further, there is now a direct coupling between the technical issues and the organizational issues. Therefore, both problem and risk management are required of the decision makers to be successful at using information technology in this way, and the decision process will need to reflect that fact.

As we expand the environments of interest even wider to surround the whole business, it is easy to see that the decision process needs to be led by risk management instead of by problem management. The decisions most often taken at this level of the organization concern risks, as it is the future instead of today that is trying to be influenced.

In our experience, few organizations actually use risk management as they increase their use of information technology. Instead, they continue to try to apply problem management. This is why I believe that few companies actually get very much value from their information technology. Paul

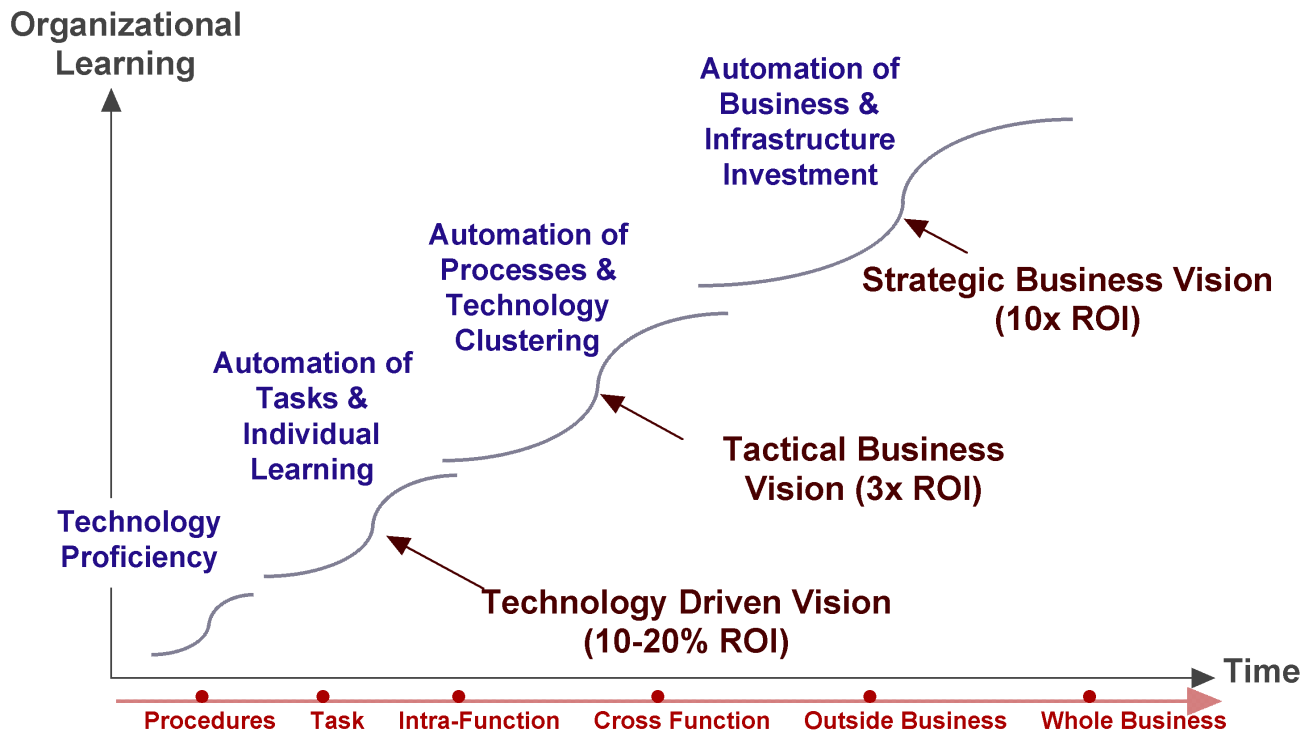


Figure 4. IT Learning and Usage Pattern

Strassman's studies concerning which organizations create the greatest business value out of their computing supports this notion as well.¹⁵

It can readily be seen that if a risk management (or taking) ethic (i.e., the application of explicit risk management) does not exist across the organization, there will always be something (i.e., informational, temporal, or control considerations) left out of the decision making process. Furthermore, it is critically important that a way be found to get risk management started at the top of an organization, and not just from the bottom for exactly this same reason, as the experience in the quality field has demonstrated.

Risk Management Context, Perspective, & Process

I have tried to describe the situation that occurred in the above discussion in Figures 5 and 6. Turning to Figure 5 first, the three axes have been labeled as process, another context, and the last as perspective. These axes create the totality of what needs to be considered in the application of risk management.¹⁶

The process axis concerns the decision process that an organization or individual uses, such as that discussed in Figure 3. The context axis concerns the specific circumstances that are in question. Context is very important, as it circumscribes the boundary or environments of interest involved in the decision process, as well as time of the situation. The last axis concerns perspective, i.e., who is making the decision, for a specific risk

¹⁵ See Strassman, Paul, *The Business Value of Computers*, Information Economics Press 1990. Strassman shows that there is no link between information system investment and profit. The organizations that seem to benefit most from using computers are those that use them to increase the value of management, i.e., improve management's decision making capability.

¹⁶ Temporal, control and informational considerations are embedded within these axes—for example, process links to control, information links to context, while information, control, and time link to perspective.

may appear very different in severity and likelihood to one person than to another. The difference is colored by one where resides (internal to an organization or external to it), as well as by experience. It is important that each of these three axes be defined to understand a risk fully.

Turning next to Figure 6, you can see that the space defined by the three axes has been divided further into three layers corresponding to the three information system utilization visions earlier illustrated in Figure 4. Notice how each vision expands the domains of the decision process, the context, and perspective involved.

For instance, as we move say, from a technical driven vision to a tactical business vision, the decision process needs to expand the number, types, and kinds of decision making techniques required to address the new context. Project managers deal with issues at the technical driven vision level that are different from those being dealt with by middle-level managers at the tactical

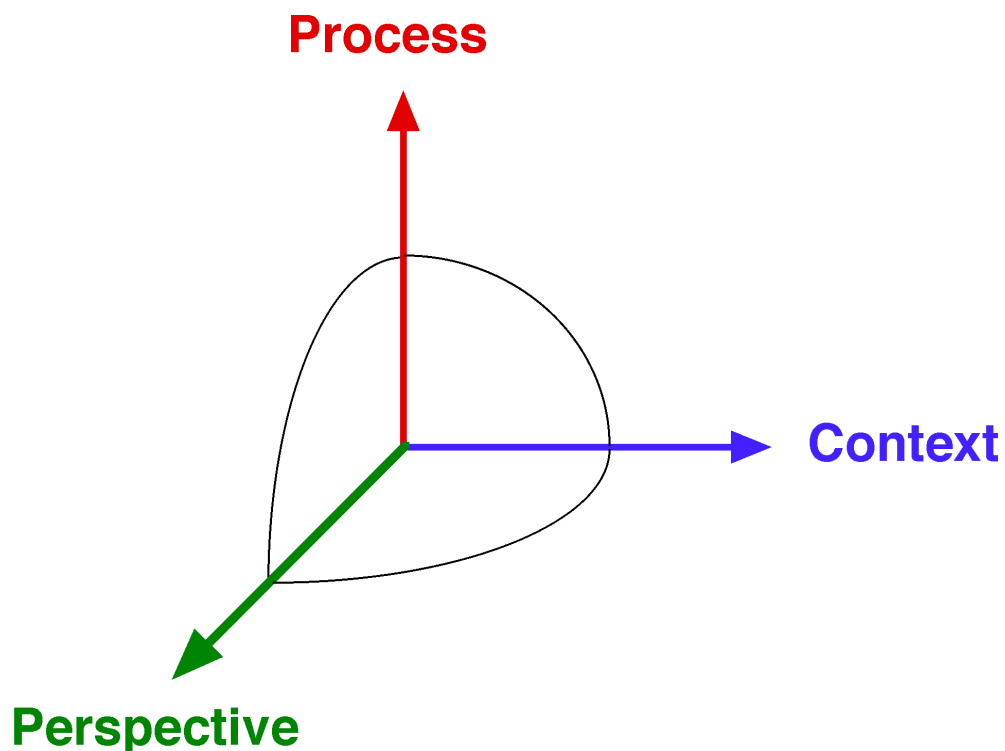


Figure 5. Risk Management Elements

business vision level, for example.¹⁷

As one moves up the organizational hierarchy the context, perspective and underlying decision-making process required is modified. This becomes clearer when one examines the different types of decision-making techniques used at different levels of the organizational hierarchy. As shown in Figure 7, senior decision makers tend to use intuitive methods the most, while those involved in program level decisions use heuristic-based procedures, whereas for project level decision makers analytical techniques rule.¹⁸ You can see that the techniques applied relate directly to their organizational perspective,

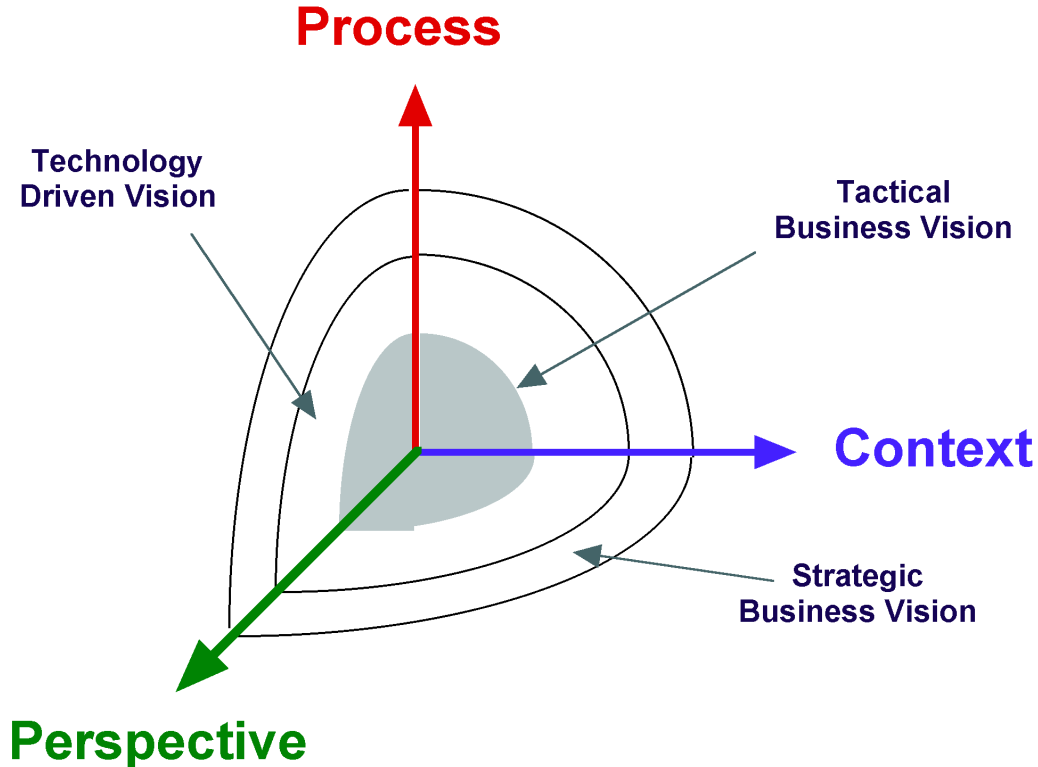


Figure 6. Management of Risk Elements

¹⁷ It should be obvious that the boundary isn't as static as defined or is depicted. The "volume" described by a particular decision is constantly shifting in shape as other actions are being taken.

¹⁸ Notice the overlap. All the approaches are used somewhat at each organizational level but certain ones dominate. Organizational culture also influences the decision taking methods used as well, with intuitive approaches often being used by small, entrepreneurial firms. A well-run organization has all three types operating in balance (see the small area of overlap).

as well as those regarding the domain of issues they are most concerned with.

Notice in Figure 7 that we have further divided the three perspectives along the lines of risk engineering, risk transformation, and risk administration. The reason is each different level of an organization views problems and risks unequally. At the lower levels of the organization, where analytical risk approaches are used, the handling of risk is (or at least, should be) more administrative in nature. The domain of interest is well defined and is inward looking. Little doubt should exist. In contrast, the domain of interest for senior managers is very wide, spanning not only the internal organizational domain, but also the external world as well. The job of senior management is to deal with risk, i.e., to engineer both the internal risks and external risks to the organization's best advantage. Middle levels of the organization must transform the risks accepted into opportunity for the organization, i.e., they must turn and direct the aspirations of the organization into some concrete course of action.^{19,20}

The above model does, of course, assume that there exist some tangible or “organized” risk management culture that is operating throughout the organization. If one does not exist, meaning that the organization is fundamentally a problem solving organization, the lower levels of the organization will be left trying to solve problems and resolve risks for the organization as a whole. We have found that this tends to happen, especially when information systems developments are concerned. The reason is that most senior and middle management executives are not comfortable with information systems technology, and therefore, they pass decisions

¹⁹ Returning to table 1 one could just as easily substitute Chief Executive Officer (CEO) for risks, and project manager for problems, and accurately describe the domain each operates in.

²⁰ Risk engineering, risk transformation and risk administration are together analogous to total quality management, quality assurance, and quality control. Each covers a larger scope

concerning its application down the organizational chain to the projects to make. There has been some movement to change this, as it is becoming clear that, as one CEO put it to us, “he has turned over his company to the programmer.”²¹

The Decision Process As Communication Channel

From my experience, the “glue” that allows risk management to operate throughout the various organizational levels is the quality of the underlying decision-making process used by the organization. The US Army, on the operational side, for example, uses a standard operating procedure for making decisions that is followed from the platoon level to the Army Chief of Staff. This approach, has a basic four-stage decision process called the METT: mission, enemy, terrain (and weather), and troops available.²² This simple decision model is used at each level of the operational forces, from the platoon leader to the Chief of Staff.

When used by a platoon leader, the concern (i.e., context) is the 200 meters of front. He tailors the METT to concentrate on the mission he is given, taking into account both his perspective and that of his immediate senior. He begins by comparing his mission against the known capability of the enemy to keep him from accomplishing his mission (i.e., another perspective view).

He then analyses the risks involved in the terrain and weather that might hinder his mission, both alone and given the risks that the enemy poses. Alternatives and consequences are compared.

than the other, each provides a different perspective on the situation, and each uses different but related techniques to accomplish their goals.

²¹ An interesting facet of organizations that do not have strong risk management, senior management has very little room in which to make decisions. By the time a decision is ready to be made by them, they are in a sense “boxed in” by decisions of their sub-ordinates and staffs. For more detail, see *Command Decisions*, Kent R. Greenfield, ed., USGPO, 1959 and Nils Brunsson, *The Organization of Hypocrisy*, John Wiley & Sons, 1989.

The platoon leader next analyses whether he has the troops available and the capability to complete the mission (i.e., performance risk). When the analysis is complete, a troop order (i.e., risk action plan) is created that details the actions to be taken by the platoon, and what actions need to be taken if things change.

Now, what is interesting is that this same process has been followed at each level of the operational hierarchy. When the order has reached the platoon leader, the risks (and opportunities) have been identified and assessed (at the level of granularity demanded by the specific organizational level).

If you were to check at each level above the platoon leader, you would see that as the mission area or domain of decision making has expanded (for instance, a battalion commander might have to worry about 2 to 20 kilometers of front instead of 200 meters), the basic METT analysis would stay the same. However, the types of analysis tools and techniques would have changed. Capitalization and performance risks (i.e., the number and types of troops required to complete a mission) would be a prime concern, as it is for a program manager. Because the decision-making domain has increased, more organizational units would start to become involved (for example, artillery, logistics, administration, intelligence, etc.).

You would also find that information from the platoon leader would have been captured and sent up for use for decision making at this level. By using the METT, the appropriate information in the right format can easily be acquired for use. Further, the reasons why something worked and something else did not can be understood, analyzed, and become part of the organizational learning set.

²² The METT is sometimes written as METT-T. The last “T” stands for “time.”

If you were to check on the Chief of Staff, you would again find the basic principles underlying the METT being used, but the actual process would be tailored to support the vast decision making environment that the Chief of Staff is involved in. Additionally, it is possible (at least in theory) to trace a decision from the Chief of Staff down to the platoon leader, and conversely, from the platoon leader back up to ensure that there was: (1) no disconnect between policy given and actions taken, and; (2) that the capital provided supported the performance required.

The military has found out that proactive management of risk is required for, if no other reason, personal survival on the battlefield. The penalties for not proactively managing risk are severe and quick. If you do not, you rarely get a second chance to practice it.

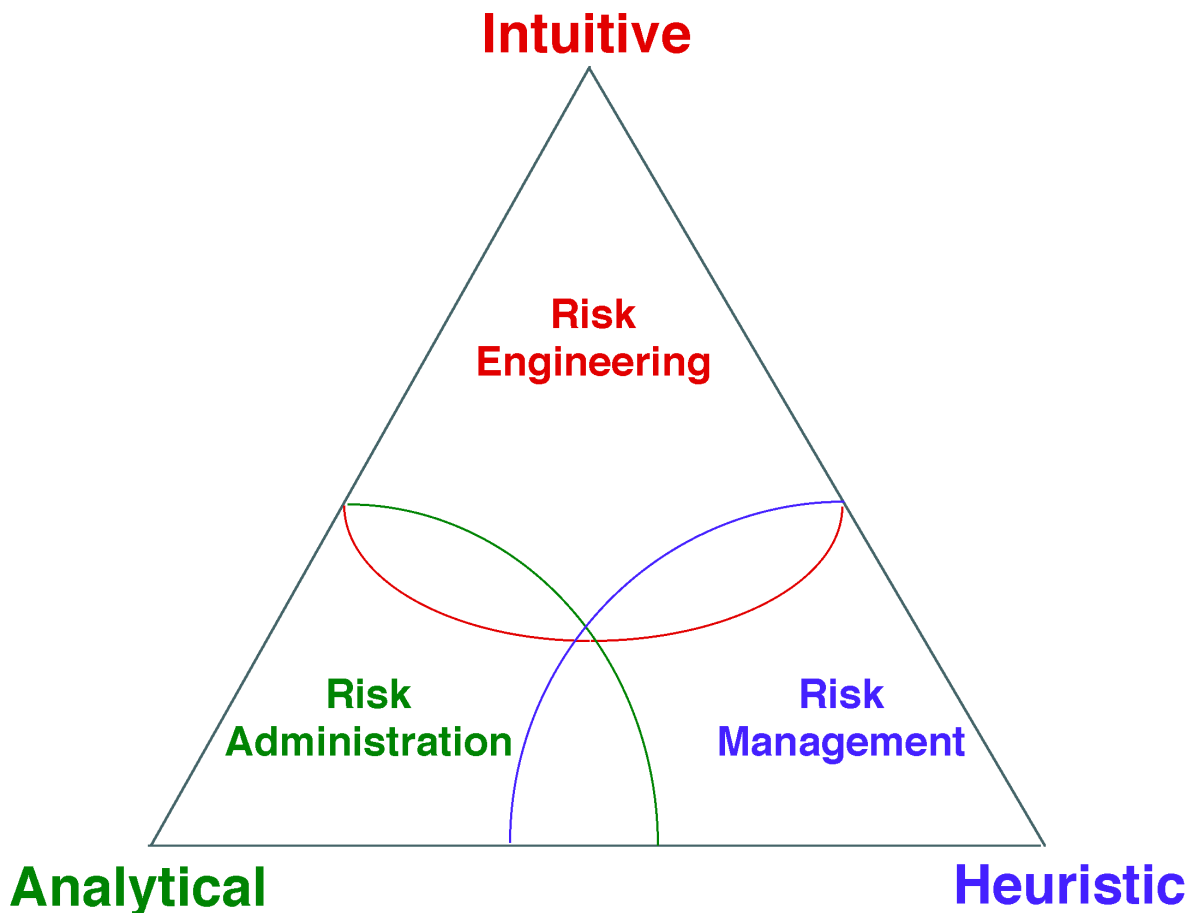


Figure 7. Organization Management of Risk Approaches

The METT approach (which resembles the total quality management technique of creating repeatable, measurable, and visible processes) ensures consistency and continuity throughout the service, especially in the allocation of resources. Furthermore, it allows risks and problems to be separated and dealt with in a very effective manner. As the environments of interests increase, i.e., the area of military operations expand, the base process remains the same, but more organizational units become involved to handle different types of issues, such as intelligence, logistics, etc.²³

I have found the same types of decision processes exist in companies like Royal Dutch Shell, Intel, HP, among others, which have a very strong risk management ethic throughout their organizations. In Shell, for example, the decision process is very well understood and followed. It becomes modified for different organizational levels, but generally, a consistent and understood process is used. At board level, decisions to make major changes from the norm must be unanimous to pass. This reflects a view that the decision must be “obvious” to everyone, otherwise a flaw is assumed in the data or decision process.²⁴ Shell also works very hard to ensure that the process does not become too bureaucratic or stifling, which is a danger if care is not exercised. They achieve this by constantly trying to improve it.

This same approach to managing risk can be found within the CYNIC® Risk Engineering Framework Methodology.²⁵ In CYNIC, we have created a

²³ We should note that the decision process becomes more important (and more closely followed) as the situation becomes more critical and/or complex. In less critical or complex situations, the process is generally followed but often short-circuited.

²⁴ The unanimous approach to making critical decisions is one that was used in W.W.II among the allies, and was found effective in ensuring consensus. Japanese organizations also use this consensus approach in making their decisions. For more on Shell, see, William Sheeline, “Shell Gets Rich by Beating Risk,” *Fortune*, 26 August 1991.

²⁵ CYNIC® is a registered trademark of the ITABHI Corporation. Although CYNIC was originally aimed at managing the risks in utilizing information systems, it has been

means to instill a risk ethic that can be shared throughout an organization. CYNIC implements the three axes shown in Figure 5 by developing a standard decision process that can be modified depending on the context and perspective of the decision maker within the organization (from senior executive to software designer or programmer). Different risk management techniques are also supported to allow the decision-maker to use the most appropriate technique for the situation encountered. The CYNIC process can also be used for “proactive” problem management, i.e., problems do need to be dealt with, and the best way to ensure that the future is considered in problem analysis is to embed risk management into that process from the very start. Thus, a decision-maker can use CYNIC for either risk or problem management.

To aid in overcoming the decision boundary limits that organizational hierarchy often imposes, we have developed what we call the FITRE™ database.²⁶ In the database are lessons learned from other organizations on how to identify, analyze, and manage risk, be it business or technical. By being able to access a database, lessons learned and other types of information can be shared by decision-makers across the organization, allowing decisions and questions of risk to be framed within the proper context.

The approach to risk management found in CYNIC allows a linkage between business strategy and operational strategy to be formed, as senior level decisions can be traced from the top of the organization to the bottom, and back up again. In other words, having a consistent process and a database of lessons learned (i.e., the organization's history) allows risk knowledge and

broadened to manage risks in a wide range of domains, such as business management, strategic planning, acquisition, etc.

²⁶ FITRESM (Forensic Information Technology Risk Engineering) database is a service mark of the ITABHI Corporation.

actions to be shared and communicated in a common language throughout the organization. This is critical if the organization is to act as a whole, instead of disparate parts. The approach also allows the communication of risk downward throughout the organization, as well as for risk to be communicated upwards.²⁷

Most importantly, CYNIC attempts to create a philosophical underpinning of not only performing risk management, but a culture of managing risk, whatever domain it was created in. In other words, CYNIC spans the entire organization in its use of information technology. Issues of political risk, organizational risk, technical risk, financial risk, societal risk, etc., are all bound into the process. This is critically important given the fact that many applications of information systems can have severe social (and therefore legal) impacts when they do not work well.²⁸

Elements of CYNIC have been incorporated within numerous organizations' information technology project and program management and development models, such as the Software Productivity Consortium Evolutionary Spiral Process (ESP), which is based upon Barry Boehm's spiral model of software development.²⁹ Both ESP and Boehm's spiral model are aimed at creating risk management-based approaches to software development, and are based

²⁷ It is important to note that risk communication must travel in two directions. First, it must travel from the top down, in order that the objectives of the organization can be effectively sought. However, it must also flow upwards, to allow senior management to understand whether the objective sought can actually be obtained with the means of execution available. The paradigm of flow is objective → strategy → tactics → means of execution → tactics → strategy → objective. If the flow is solely in the upward direction, then the initial information, time, and control boundaries encountered will always limit risk communication.

²⁸ See Peter Neumann's bi-monthly listing of "what has a computer done to you lately," in his column, "Risks" in the *ACM Software Engineering Notes*.

²⁹ See Boehm, Barry, "A Spiral Model of Software Development and Enhancement," *ACM Software Engineering Notes*, August 1986, pp. 14-24.

upon an iterative four stage decision model that controls actions in developing software.³⁰

The importance of having a defined decision process for creating a risk ethic and fostering communication of risk within an organization should not be underestimated. If the vocabulary is not in place to talk about risk, if there is not a means to decide about what actions should be taken when faced with risk, and if there is no previous history from which to learn and therefore adapt, then risk management will not take hold within an organization.

Summary

In the paper I have tried to describe some of my experiences from performing risk management, especially the problems involved in getting people to apply it correctly and why they don't. In my experience, few organizations, especially those within the community served by the SEI, practice risk management in any formal sense. When it is applied, it is inevitably based on a tool and used at the lowest level of the organization (typically a project). From my experiences so far, I also see that the introduction of risk management into organizations will likely follow the route that quality management took, i.e., it will flow bottom-up throughout the organization. This is unfortunate, since as the quality management practitioners discovered, this path raises expectations that cannot be met, the process itself is blamed unfairly for any difficulties encountered instead of how it was implemented, etc. I believe that unless a top-down approach, one that is based on an underlying decision management process, is created and used

³⁰ This has not been universally recognized, however. Again a case of technique overshadowing a process. The first stage determines the objectives, alternatives and constraints available, the second stage evaluates the alternatives, the third stage develops and verifies the next-level product, and the final stage is to plan the next phase of development. One can compare these four stages to the six depicted in Figure 3 and see that they are in fact almost identical in result.

with the bottom up approaches which seem more natural, then the same, long, tortuous path that quality management followed will also be the fate for risk management. Old lessons will, unfortunately, likely have to be relearned.

The key is to realize that the management of risk is about the management of change, and the choices that come with change. The longer this fact is ignored; the longer organizations will take to gain the benefits of risk management.

This article first appeared in the Proceedings of the 2nd Software Engineering Institute Conference on Risk Management, 2 March 1993, Pittsburgh, PA. Copyright © 1993 ITABHI Corporation. All rights reserved.