INTEGRATED RISK MANAGEMENT

Final Report
NASA/ASEE Summer Faculty Fellowship Program - 1993
Johnson Space Center

Prepared By:	J. L. Hunsucker, Ph.D., P. E.
Academic Rank:	Associate Professor
University & Department:	University of Houston Department of Industrial Engineering, Houston, TX, 77204 - 4812
NASA/JSC	
Directorate:	New Initiatives
Division:	Planning and Strategy
Branch:	N/A
JSC Colleague:	Lyn Gordon - Winkler
Date Submitted	August 2, 1993
Contract Number:	NGT 44 001 800

ABSTRACT

The purpose to this report is to first present a basis or foundation for the building of an integrated risk management plan and then to present the plan. The integration referred to is across both the temporal and the hierarchical dimensions. Complexity, Consequence, and Credibility seem to be driving the need for the consideration of risk. Reduction of personal bias and reproducibility of the decision making process seem to be driving the consideration of a formal risk plan. While risk can be used as either a selection tool or a control tool, this paper concentrates on the selection usage. Risk relies on stated purpose. The tightness of the definition of purpose and success is directly reflected in the definition and control of risk. Much of a risk management plan could be designed by the answers to the questions of why, what, who, when, and where. However, any plan must provide the following information about a threat or risk: likelihood, consequence, predictability, reliability, and reproducibility. While the environment at NASA is seen as warm, but not hot, for the introduction of a risk program, some encouragement is seen if the following problems are addressed: no champion, no commitment of resource, confused definitions, lack of direction and focus, a hard sell, NASA culture, many choices of assessment methods, and cost. The plan, itself, is designed to follow the normal method of doing work and is structured to follow either the work break down structure or a functional structure very well. The parts of the plan include: define purpose and success, do initial threat assessment, do initial risk assessment, reconcile threats and parameters, put part of the information down and factor the information back into the decision process as it comes back up, and develop inferences. Two major suggestions are presented. One is to build an office of risk management to be used as a resource by managers in doing the risk process. Another is to form a pilot program to try out the details in the plan and modify the method where needed.

INTRODUCTION

Decision making is becoming more and more difficult as the complexity of society increases and the consequences of bad decisions become more severe. Factors such as these force the consideration of risk into the decision making process. In truth, good managers have always considered risk in their decision making. However, if personal bias is going to be minimized and if the decision making, at least in the consideration of risk, is to be standardized enough to be reproducible by another analyst, then the process must be formalized. Therein lies the basic fundamental purpose of this report., the formalization of the consideration of risk in technological decision making.

Risk, oftimes in the past, has been only considered in the areas of cost, schedule, performance, or safety. The concept of risk is significantly greater than this. In today's society, risk comes from many different sectors such as political risk, societal risk, environmental risk, underfunding risk, just to name a few. The trap here is that we all have a tendency to give the most consideration to those things which are easily measurable, like schedule and cost performance. This is rather similar to the concentration in manufacturing, at least up through recent times, on direct labor in cost reduction even though direct labor usually accounts for around 20% of a products cost while indirect labor and materials cost split the remaining 80% between them. Direct labor is easy to measure. Schedule performance is easy to measure. While both are important, they are not the only important things. Risk management must be as broad as possible.

PROBLEM STATEMENT

The intention of this report is to begin the development of a formalized process of decision making in risk management that is integrated both through the life cycle of the entity at risk and also integrated through the hierarchy of the organization. Part of accomplishing this task will be to develop consistent terms and to formulate a plan that has a reasonable chance of being implemented on a broad basis. As an additional consideration, this report should serve as a beginning point for a follow-on work in risk management.

TERMS AND ASSUMPTIONS

Entity - refers to the program, project or thing to which the risk management program is to be applied.

Threat - Any real or perceived threat against a stated purpose. Threats are not necessarily measurable.

Parameter - A measurable quantity with an acceptable and an unacceptable region and perhaps a gray region. The totality of parameters, if all are in the acceptable region, should reflect that the purpose of the entity is fulfilled or being fulfilled.

Risk - This term is used in two different ways. One is the familiar meaning from everyday life and expresses the likelihood that an unfavorable event will occur. The other is a technical definition and says risk is the mathematical expectation of the parameter in question. Under this definition, risk is a product of likelihood and consequence.

Risk management - Different authorities have defined this slightly differently. Our definition will be that risk management includes risk or threat identification, quantification, inferences, control, and mitigation.

Prodrome - a warning event or sign.

DISCUSSION OF THE LITERATURE

The literature is very extensive on risk management. A quick glance at a paper written by Garland Bauch (unpublished) on Integrated Risk Management shows a discussion of risk management in fourteen different industries that ranges all the way from the construction to the finance industries. There are virtually thousands of papers on risk management in the literature. Many of these papers deal with either safety or with quantification techniques. Here and there, scattered among the rest, are a few which either concentrate on risk identification or provide an overview.

Fortunately, the reading of four or five pieces will provide the interested manger with an adequate background to pursue consideration of risk management. Start with NASA Management Instruction 8070.4 on Risk Management Policy for Manned Flight Programs (effective date Feb. 3, 1988). This document shows that

NASA has been trying to formalize its risk policy for quite some time. Then move to a set of papers by R. G. Batson. One is Risk Analysis Methodology Survey, done as part of the NASA/ASEE Summer Faculty Fellowship Program in 1987 and a follow on piece by the same author, Program Risk Analysis Handbook, 1987. These two will give somewhat of an overview and a fair amount of information on quantification methods. From here, a reading of Bauch's work (available from either me or the author) will provide a nice overview of the literature. This literature review is particularly strong in the risk identification areas. Finishing off with the Defense Systems Management College's manual, Risk Management, Concepts and Guidance, will provide an overview of the entire risk management process. The reader who is pressed for time can do no better than concentrate their efforts on these last two, Bauch's work and the DSMC's manual.

BACKGROUND

Why is this a problem?

The first step in designing new methodology is to determine what problem the new methodology is aimed at solving. In problem solving, the definition of the problem is perhaps the most important and crucial step. Here, this step becomes even more important since the identification of the motivators will, or should, give some indication of the feasibility of introducing a new methodology.

Based on interviews with NASA managers, there seem to be three factors forcing the consideration of a risk management program: complexity, consequence, and credibility. Decision making is becoming significantly more complex. As technology becomes more complex, so must the decisions that shape and mold technology. There is more to know, more to consider, and more to affect a technological decision than ever before. Meanwhile, there may be less resource to enact a decision. So complexity is growing. The consequences of technological decisions have become significantly greater. A wrong decision can have a multi billion dollar impact or even wipe out a whole agency or company. Faced with increasing complexity and consequence, the modern manager is faced with showing upper level management that a good job has been done in the decision making. Some means has to be established to demonstrate credibility. So complexity, consequence, and credibility are driving the consideration of risk.

Since all good managers have always considered risk, the next issue becomes one of why should the program be formalized. One reason is the reduction, or at least the realization, of personal bias. Everyone has their own unique view on risk taking. Some people are risk takers and some are risk avoiders. In decision making, some method must be used so that the other players have some idea of the risks being taken. Another factor pushing formalization of risk management is reproducibility. First, different decision makers should be able to arrive at close to the same decision on risk. Second, the decision process should be reproducible by another analyst. This is required in order to insure that the decision makers are in accord on the treatment of risk. In many industries, and NASA is no exception, managers change jobs rather frequently. Having reproducibility in the risk decision process should help to provide continuity through this management change.

In summary on why should the issue of a formalized risk management program be addressed, perhaps the best answer is that managers are being forced out of their comfort zones. There seems to be a significant amount of managerial unrest and, in some few cases, even paranoia. There is a basic difference between a bad decision and a wrong decision and managers understand the distinction. A bad decision is one based on a faulty decision making process. A wrong decision has a good process which considers everything which should be considered but arrives at a conclusion that leads to difficulty. Most often this difficulty could be that a consequence with a small probability was realized. All of this forces managers out of their comfort zone. Decision making has gotten harder.

Different Aspects of Risk Management: Selection and Control

There are two different uses of risk management. One is to consider risk in the selection among alternatives. In this usage, a manager is considering several different alternatives and uses risk as one criterion to choose a favored alternative to pursue. The other use of risk management is in the control mode. Here an alternative has already been selected and is being pursued. Then the risk must be managed and controlled to ensure that unfavorable consequences do not occur.

As an example, one might consider risk in choosing among different types of propulsion systems. There certainly will be other factors impacting the choice but risk will be one of the factors. This is risk management in the selection mode. Once a propulsion system

is chosen, then risk must be controlled as the propulsion system is designed, manufactured and operated. This is risk in the control phase. As is obvious, the selection mode comes first in the natural development of tasks and then the control mode. As a rule, less will be known about risk in the selection than in the control mode due to the absence of data.

Most of the literature deals with risk in the control mode. There is little distinction in the readings between the two fundamentally different uses of risk management. Since beginning at the beginning has a large amount of appeal in a logical development of a process, this report will concentrate on the selection mode of risk management. However, it is felt that the transition from the selection to the control mode will be natural and relatively easy.

Risk Relies on Purpose

A basic fundamental issue with risk management is the determination of what is at risk. To this end, the entity in question must have a defined purpose. Otherwise there is no way to rationally discuss risk because one cannot answer the question of what is at risk. The tightness of this definition of purpose, to a large degree, determines how tight the risk management can be. Said another way, the strength with which the task is known and understood will be directly reflected in the strength that the risks and threats against a task are understood.

A trap here is the sophomoric attitude that everyone knows and understands safety, cost, and schedule and this is what is at risk. These are just parameters that reflect threats against the basic purpose of the entity. There are no doubt other threats that are not reflected in these parameters. If one does not know the fundamental purpose of an entity, then any discussion of risk can only be at a most superficial level.

Related to this discussion of purpose is the definition of success. If you know the purpose, then you should be able to decide what you consider to be success. If you cannot do so, then, again, risk consideration is, at best, only superficial.

The Real and Perceived Dimensions of Risk

As the definition of success changes, then what is at risk changes and so must the way that risk is managed change. This

thought leads to two major dimensions of risk management and two quasi dimensions of risk management.

As a project or program moves through its life cycle, how success is defined changes. Consider the Shuttle. Before the first flight one major goal was to prove that the design was flight capable. Now that the program has matured, that goal has already been established. Thus the definition of success has changed. Therefore what is at risk has changed and risk management must also change. So risk management has a temporal or time dimension.

The manager at the very lowest level of an organization clearly has a different definition of success than the manager at the very highest level. There will be some commonalty between the two, but there will also be major differences. This means that risk will be different between different levels of an organization. This leads to the hierarchical dimension of risk management.

A minor dimension of risk management is imposed by the consideration of contractors. The way that the contractor views success and the way that the parent organization views success are different, therefore the risk management is different. Another minor dimension is induced by the matrix structure used in many organizations. At NASA, for example, projects and programs are going to view success differently.

So there is a temporal, hierarchical, contractor, and matrix dimension to risk management. The trick is to integrate the management of risk across these dimensions.

The Five W's: Why, What, Who, When, Where?

Much of the above discussion in risk management can be reduced to these five questions.

Why? - Why do a new program such as this?

What? - What is at risk? What is the purpose of the entity?

Who? - Who is at risk, NASA or the contractor?

When? When in the life cycle of the entity is the risk to be managed?

Where? - At what level in the organization is the risk to be considered?

The answers to these five questions will certainly shape a proposed risk management program.

Required Information About A Risk or Threat: Likelihood, Consequence, Predictability, Reliability, and Reproducibility

Once a risk or threat has been identified, the next question is how much information is needed on the threat to factor risk into the decision making process. Likelihood refers to the probability that an unfavorable event will occur. Consequence refers to the outcome or impact of this unfavorable event. These are usual pieces of information associated with risk. Not so usual is the consideration of predictability. Will there be conditions which forewarn the decision maker that an unfavorable event is about to occur or will the event come in an unpredictable or unheralded manner. Predictability relates directly to the amount of control that the manager will have.

Reliability refers to the underlying data or experience that the analyst is relying on to assess the threat. Has there been a lot of experience with threats of this type before? Is there a large data base that is used to assess this threat? Is this a unique experience that has never occurred and one with which no one has much exposure? Is the threat assessment a scientific assessment or is it a reasoned guess?

Closely related to reliability is reproducibility. Would another analyst be able to arrive at the same assessment? Would the same analyst, at a later date, be able to arrive at the same assessment? Reliability and reproducibility are both related to the removal of personal bias from the decision making process. Information on both of these issues is essential to the decision maker.

The Environment

If a program of this sort is being considered, then an assessment of the environment is in order. At NASA, the readiness to accept a program of this sort could at best be described as luke warm. On the negative side, almost no resource has been committed to doing integrated risk management. If the reader is tempted to believe that the rational for this is that the information or the requirement is new, go back and look at the date on the NMI 8070.4 which is 1988 or at the date on Batson's work for NASA which is 1987. There seems to be no great motivation to do risk management at any significant level above the consideration of safety, or any significant catalyst which would increase the desire to accept formal risk management as part of the decision making process. Risk management could at best be described as one of those things that managers feel that they really should do but which they are not ready to commit time or resource to doing.

On the positive side, there seems to be a growing interest in risk management. More than likely, some innovative organization at

NASA will pioneer the use of risk management in decision making and this will open the gates for other organizations to follow. There also seems to be some small indication of interest at upper levels.

Problems

The following is a short list of the perceived problems with implementing a risk management program. For the most part, they are self-explanatory.

1. No Champion - There is no champion, as yet, high enough up in the management structure or respected enough to get others to sign on.
2. No commitment of resources - There does not seem to be any large amount of resource devoted to this issue. To institute a program of this sort will require time, manpower, and money.
3. Confused definitions - Different people have used the terms differently. Many feel they have an adequate risk management program since they do a good job on safety.
4. Lack of direction and focus , absence of overview and strategy - There seems to be a real question about some of the fundamental programs of the agency such as the shuttle and the space station. This in term leads to questions about the fundamental purpose of the agency. Integrated risk management is strongly related to overview and strategy and requires a sense of direction and a tight focus.
5. This will be a hard sell - A program of this sort will change the fundamental way that manager do their business of making decisions. Most of the managers at NASA are older and have established work practices. Getting them to change may be quite difficult.
6. The NASA culture presents a problem - Typically, NASA would assign this problem to a contractor and expect the contractor to bring back a finished product without NASA having much input or doing much of the development on the system. This seems to be the predominant approach used to this point. As a management style for solving problems of the sort discussed here, this, at best, will lead to mediocrity.
7.. Abundance of choices for risk assessment and quantification - There are a large number of methods developed in other agencies and industries to quantify risk. The large amount of choice increases the difficulty of the decision.
8. Cost - As mentioned earlier, a program of this sort will require the expenditure of resource and time. Training must occur in

the usage of such a program.. Tools must be developed. The cost expenditure to introduce integrated risk management throughout the agency would be significant.

RISK MANAGEMENT PLAN BASICS

As stated before, the plan presented will concentrate on the decision mode of risk management as opposed to the control mode. If the process works well at the beginning during the decision phase, then it should evolve handily into the control mode thus providing for temporal integration.

Any plan for risk management must follow the normal way of doing work where possible. For this reason, the plan presented follows the work break down structure or the functional analysis structure equally well. This plan should adapt well to what ever method is used to break down design work into manageable pieces.

Since one of the most difficult parts of risk management is identification, this plan separates risks from threats. Recall that risk is determined by looking at measurable parameters and determining their mathematical expectation. Threats, on the other hand, may or may not be measurable.

THE PLAN

Step 1: Define Both Purpose and Success- The first part of this step is to define the purpose. Recall that the tightness of this definition determines how well focused the risk management plan will be. The second part of this step is to define success. The end result of step one will be two paragraphs, each containing one or two sentences. The first paragraph will be a simple statement of the purpose or function of this entity. The second paragraph will be a sentence that starts, "This entity will be successful if ...". The intent here is to tie success and purpose together in order to assist in focusing the work. This purpose follows the risk management information as it flows down through the organization.

Step 2: Do Initial Threat Assessment -

1. List the threats - Every single threat against the fundamental purpose or function should be listed. Their importance can be decided later. As young doctors learn in medical school, if you don't consider the diagnosis, then you won't make the diagnosis.
2. For each threat, discuss the likelihood. This is done in paragraph form and may or may not include an actual probability.

3. For each threat, discuss the impact or severity should this event occur. This also is done in paragraph form.

4. For each threat, list the prodomal events - The intent with this step is to list the conditions or warning signs that would signal that the threat is about to be realized. This step serves at least two purposes. One, it helps to establish credibility in that the threat has been thought about enough to identify those events leading to a crisis. The other purpose is that it helps the manager to evaluate the strength of the threat and the uncertainty associated with the threat.

5. For each threat, discuss the reliability of the threat assessment. - Identify the basis of the assessment. Give some indication of the strength with which convictions are held.

Step 3: Do Initial Risk Assessment -

1. Determine which parameters to measure - This will not necessarily be an easy task. A good starting place is in the DSMC manual in chapter 3. They start with Technical Risk, Programmatic Risk, Supportability Risk, Cost Risk, and Schedule Risk. The intent here is to identify a broad enough set of parameters such that if they are all in an acceptable region, then the purpose of the entity is, or will be, fulfilled.

2. Develop Measurement/Assessment Methods - This step is, more than likely, going to require some outside assistance. There are numerous methods and most rely on fairly sophisticated statistical methods.

Step 4: Reconcile Threats to Parameters and Conversely - Each threat should be reflected in the parameters and each parameter should be reflected in the threats. If not, then control will be difficult to establish. It may be impossible to find a parameter whose measurement will imply some sort of control or information about a given threat. In this case the threat is moved to a Critical Threat List. Items on the Critical Threat List deserve special attention. They are items surrounded by uncertainty and typify the concept of threat in its rawest form.

Step 5: Down and Back - As the work flows, so flows the risk information. When the work is passed down the organization to the next level of management, the stated purpose is also passed in two forms. One is the upper level purpose. The other is the purpose which is appropriate for this next lower level. This level then does steps 2,3, and 4, i.e., threat assessment, risk assessment, and reconciliation including the Critical Threat List. This is then passed

up the organization for incorporation into their risk model. In order to insure that all relevant threats are identified, it is important that steps 2,3, and 4 be done by the upper level before passing the problem on down to the lower level. If the upper level just waits on lower level information, there is a greater chance that some threat to the program will not be recognized.

Step 6: Develop Inferences - This step relates to the decision making process once all the data is in. The question is one of how threat information will be factored into the decision process. Formal explanations are required at this step if the decision is to be reproducible at a later date.

IMPLEMENTATION

There seems to be two basic ways to implement this program. One is to implement it agency wide. Another is to work a pilot project and iron out the problems and then to go to a wider implementation. Of the two, I would certainly prefer the latter. There are some significant questions that must still be answered but can only be answered in implementation. How much time is required to do a program of this sort? How much resource is required? What form should the data be presented in? These and others require a pilot program.

One concept that is not necessarily clear to NASA but is clear to me is that some sort of support office is going to be required for a program of this sort. Risk assessment requires sophisticated statistical analysis. Most managers at NASA do not have the required background nor do they need it. What they do need is the ability to interpret the statistics generated. This is rather similar to their use of computers. They do not need to be a programmer, but they do need access to some resource on computer programming. In a similar manner, this office could serve as a resource of methods in risk analysis. Another use of the office would be to serve as a storage house of information. A trap here is that some individuals might perceive that this office is intended to do the risk assessment work. This should not be the case. The purpose of the office is to serve as a resource to help the manager do the work.

WHERE TO FROM HERE?

Change Management - Managing change is difficult. The reader is encouraged to read some of the work on change management listed

in the references. The amount of change that will be required of a program of this sort should not be underestimated. When a new program is going to require that work be done in a fundamentally different way, plans need to be laid on how to implement the change.

Champion - This work needs a champion, the higher in the organization, the better. Without a one it will have extreme difficulty.

Support - The support of the champion and of the agency should be both visible and tangible. Otherwise, this program will be treated as if it is just another in a long line of useless programs.

Pilot Program and Pilot Team - Ideally, a team would be formed to work on a pilot project. One possible composition for this team would be a team leader who is both a visionary and a strategist. The purpose of the leader would be to provide direction, focus, and scope to the pilot project. The rest of the team should be composed of two or more young technical types who could do the statistical analysis. The analysts on the team could provide the nucleus of the risk management office discussed above.

Structured in this way, the pilot program should be complete in one to two years. The changes in the plan should be in place by the end of that time. Then training material could be developed for a broader implementation.

REFERENCES

1. Batson, R. G., "Risk Analysis Methodology Survey", NASA/ASEE Summer Faculty Fellowship Program, MSFC, 1987.

2. Batson, R. G., Program Risk Analysis Handbook, NASA Technical Memorandum, NASA TM - 100311, MSFC, 1987.

3. Bauch, Garland T., "Integrated Risk Management", Unpublished, August 1993.

4. Defense Systems Management College, "Risk Management Concepts and Guidance", DSMC, MDA 903-87-C-0781, Ft. Belvoir, VA.

5. Hunsucker, J. L. , Shah, Jaymeen, Santos, D. L. "Strategic Considerations for Planning Major Transitions", Engineering Managemnt J., Vol. 3, , 1991.