Microsoft Solutions Framework

White Paper

Published: June 2002 For more information on MSF, see: http://www.microsoft.com/msf

MSF Risk Management Discipline v.1.1

Contents

Credits

Allison Robin, Director, Microsoft Solutions Framework

David Preedy, Program Manager, Microsoft Solutions Framework

Derick Campbell, Product Manager, Microsoft Solutions Framework

Enzo Paschino, Program Manager, Microsoft Solutions Framework

Laura Hargrave, Technical Editor, Microsoft Frameworks

Marijke Born, Release Manager, Microsoft Frameworks

Nancy Huber, Technical Editor, Microsoft Frameworks

Paul Haynes, Program Manager, Microsoft Solutions Framework

Pervez Kazmi, Program Manager, Microsoft Solutions Framework

Rob Oikawa, Program Manager, Microsoft Solutions Framework

Scott Getchell, Program Manager, Microsoft Solutions Framework

Reviewers

Brian Carter, Consultant, MCS National Practices

Brian Willson, Automotive Industry Strategy Consultant, MCS Great Lakes

David Millett, Principal Consultant, MCS NorCal

Dolph Santello, Principal Consultant, MCS Northeast

Francis Delgado Millan, Practice Manager, Microsoft Enterprise Services

Joseph Lopesilvero, Principal Project Manager, Microsoft Project Management Office

Paulo Henrique Leocadio, Senior Principal Consultant, MCS Brazil

Paulo Rocha, Principal Consultant, MCS New Zealand

Rick Varvel, Principal Consultant, MCS PacWest

Ron Stutz, Managing Consultant, MCS Rocky Mountain

Paulo Rocha, Microsoft Consulting Services, New Zealand

Anthony Saxby, Microsoft Consulting Services, UK

Ralph Schimpl, Microsoft Consulting Services, Austria

Ron Stutz, Microsoft Consulting Services, US

Brian Willson, Microsoft Consulting Services, US

Andres Vinet, Microsoft Consulting Services, Chile

Part Number: 602-i401a

Abstract

Risk management is a core discipline of the Microsoft® Solutions Framework (MSF). MSF recognizes that change and the resulting uncertainty are inherent aspects of the IT life cycle. The MSF Risk Management Discipline advocates a proactive approach to dealing with this uncertainty, assessing risks continuously, and using them to influence decision-making throughout the life cycle. The discipline describes principles, concepts, and guidance together with a five-step process for successful, ongoing risk management: Identify risks, analyze risks, plan contingency and mitigation strategies, control the status of risks, and learn from the outcomes.

Introduction

Microsoft Solutions Framework (MSF) defines a process for continually identifying and assessing risks in a project, prioritizing those risks, and implementing strategies to deal with those risks proactively throughout the project life cycle as defined by the MSF Process Model.[1]

This white paper presents the basic concepts of the MSF Risk Management Discipline which describes the principles, concepts, guidance, and a six-step process for successful management of IT *project risk.* After reading this document, a project team with experience using MSF should be able to implement a proactive risk management process for an IT project. Individuals who are new to IT project risk management should be able to understand the basic concepts, terminology, and principles required to actively participate and contribute to MSF Risk Management throughout the IT project life cycle.

While drawing upon the well-known Software Engineering Institute (SEI) Continuous Risk Management process model[2],[3] for technical project risk, MSF Risk Management Discipline seeks to interpret this model in view of Microsoft's extensive product development experience and the software development and deployment project experience derived from Microsoft Consulting Services (MCS) and Microsoft partners. MSF Risk Management Discipline extends project-focused, risk management process into alignment with enterprise IT strategy through knowledge asset recovery and tight integration with all phases of the project life cycle.

Within MSF, risk management is the process of identifying, analyzing, and addressing project risks proactively so that they do not become a problem and cause harm or loss.

MSF Risk Management Discipline has the following defining characteristics:

- It is comprehensive, addressing all of the elements in a project: People, processes, and technology elements.
- It incorporates a stepwise, systematic, reproducible process for project risk management.
- It is applied continuously throughout the project life cycle.
- It is proactive and not reactive in orientation.
- It has a commitment to individual and enterprise level learning.
- It is flexible and can accommodate a wide range of quantitative and qualitative risk analysis methodologies.

Risk Fundamentals

An essential aspect of project management is controlling the inherent risks of a project. Risks arise from uncertainty surrounding project decisions and outcomes. Most individuals associate the concept of risk with the potential for loss in value, control, functionality, quality, or timeliness of completion of a project. However, project outcomes may also result in failure to maximize gain in an opportunity and the uncertainties in decision making leading up to this outcome can also be said to involve an element of risk. In MSF, a project risk is broadly defined as any event or condition that can have a positive or negative impact on the outcome of a project. This wider concept of *speculative risk is* utilized by the financial industry where decisions regarding uncertainties may be associated with the potential for gain as well as losses, as opposed to the concept of *pure risk* used by the insurance industry where the uncertainties are associated with potential future losses only.[4]

Risks differ from problems or issues because a risk refers to the *future* potential for adverse outcome or loss. Problems or issues, however, are conditions or states of affairs that exist in a project at the *present time*. Risks may, in turn, become problems or issues if they are not addressed effectively. Within MSF, risk management is the process of identifying, analyzing, and addressing project risks proactively. The goal of risk management is to maximize the positive impacts (opportunities) while minimizing the negative impacts (losses) associated with project risk. An effective policy of understanding and managing risks will ensure that effective trade-offs are made between risk and opportunity.

Information Technology (IT) projects have characteristics that make effective risk management essential for success. Competitive business pressures, regulatory changes, and technical standards evolution can sometimes force IT project teams to modify plans and directions in the middle of a project. Changing user requirements, new tools and technologies, evolving security threats, and staffing changes all result in additional pressure for change being brought upon the IT project team that force decision-making in the face of uncertainty (risk). This is captured by the following quotation from Jim McCarthy:

> *"At virtually every stage of even the most successful software projects, there are large numbers of very important things that are unknown" (Dynamics of Software Development, 1995, p. 99).*[5]

Foundation Principles

The MSF Risk Management Discipline is founded on the belief that it must be addressed proactively; it is part of a formal and systematic process that approaches risk management as a positive endeavor. This discipline is based on foundational principles, concepts, and practices that are central to MSF. The MSF foundational principles contribute to effective project risk management.[6] However, the following principles are especially important for the MSF Risk Management Discipline.

Stay Agile—Expect Change

The prospect of change is one of the main sources of uncertainty facing a project team. Risk management activities should not be limited to a single phase of the project life cycle. All too often, teams start out a project with the good intention of applying risk management principles, but fail to continue the effort under the pressures of a tight schedule all the way through project completion. Agility demands that the team continuously assess and proactively manage risks throughout all phases of the project life cycle because the continuous change in all aspects of the project means that project risks are continuously changing as well. A proactive approach allows the team to embrace change and turn it into opportunity to prevent change from becoming a disruptive, negative force.

Foster Open Communications

MSF proposes an open approach toward discussing risks, both within the team as well as with key stakeholders external to the team. All team members should be involved in risk identification and analysis. Team leads and management should support and encourage development of a no-blame culture to promote this behavior. Open, honest discussion of project risk leads to more accurate appraisal of project status and better informed decision making both within the team and by executive management and sponsors.

Learn from All Experiences

MSF assumes that keeping focus on continuous improvement through learning will lead to greater success. Knowledge captured from one project will decrease uncertainty surrounding decision-making with inadequate information when it becomes available for others to draw upon in the next project. MSF emphasizes the importance of organizational or enterprise level learning from project outcomes by incorporating a step into the risk management process. Focusing directly on capturing project outcome experiences encourages team-level learning (from each other) through the fostering of open communications among all team members.

Shared Responsibility, Clear Accountability

No one person "owns" risk management within MSF. Everyone on the team is responsible for actively participating in the risk management process. Individual team members are assigned action items specifically addressing project risk within the project schedule and plans, and each holds personal responsibility for completing and reporting on these tasks in the same way that they do for other action items related to completion of the project. Activities may span all areas of the project during all phases of the project and risk management process cycles. It includes risk identification within areas of personal expertise or responsibility and extends to include risk analysis, risk planning, and the execution of risk control tasks during the project. Within the MSF team model, the project management functional area of the program management role cluster holds final accountability for organizing the team in risk management activities, and ensuring that risk management activities are incorporated into the standard project management processes for the project.[7]

Key Concepts

In this section, the important concepts about risk and risk management that are central to understanding the MSF Risk Management Discipline are discussed.

Risk Is Inherent in any Project or Process

Although different projects may have more or fewer risks than others, no project is completely free of risk. Projects are initiated so an organization can achieve a goal that delivers value in support of the organization's purpose. There are always uncertainties surrounding the project and the environment that can affect the success of achieving this goal. By always keeping in mind that risk is inherent and everywhere, MSF practitioners seek ways to continuously make the right trade-off decisions between risk and opportunity and not to become too focused on minimizing risk to the exclusion of all else.

Proactive Risk Management Is Most Effective

MSF adopts a proactive approach to identifying, analyzing, and addressing risk by focusing on the following:

- Anticipate problems rather than just reacting to them when they occur.
- Address root causes instead of just dealing with symptoms.
- Have problem resolution plans ready ahead of time—before a problem occurs.
- Use a known, structured, repeatable process for problem resolution.
- Use preventative measures whenever possible.

Effective risk management is not achieved by simply reacting to problems. The team should work to identify risks in advance and to develop strategies and plans to manage them. Plans should be developed to correct problems if they occur. Anticipating potential problems and having well-formed plans in place ahead of time shortens the response time in a crisis and can limit or even reverse the damage caused by the occurrence of a problem.

The defining characteristics of proactive risk management are risk mitigation and risk impact reduction. Mitigation may occur at the level of a specific risk and target the underlying immediate cause, or it may be achieved by intervention at the root cause level (or anywhere in the intervening causal chain). Mitigation measures are best undertaken in the early stages of a project when the team still has the ability to intervene in time to effect project outcome.

Identification and correction of root causes has high value for the enterprise because corrective measures can have far-reaching positive effects well beyond the scope of an individual project. For example, absence of coding standards or machine naming conventions can clearly result in adverse consequences within a single development or deployment project and thus be a source of increased project risk. However, creation of standards and guidelines can have a positive effect on all projects performed within an enterprise when these standards and guidelines are implemented across the entire organization.

Treat Risk Identification as Positive

Effective risk management depends on correct and comprehensive understanding of the risks facing a project team. As the variety of challenges and the magnitude of potential losses becomes evident, risk activity can become a discouraging activity for the team. Some team members may even take the view that identifying risks is actually looking for reasons to undermine the success of a project. In contrast, MSF adopts the perspective that the very process of risk identification allows the team to manage risks more effectively by bringing them out into the open, and thereby increases the prospects for success by the team. Open, documented discussion of risk frees team members to concentrate on their work by providing explicit clarification of roles, responsibilities, and plans for preventative activities and corrective measures for problems.

The team (and especially team leaders) should always regard risk identification in a positive way to ensure contribution of as much information as possible about the risks it faces. A negative perception of risk causes team members to feel reluctant to communicate risks. The environment should be such that individuals identifying risks can do so without fear of retribution for honest expression of tentative or controversial views. Examples of negative risk environments are easy to find. For example, in some environments reporting new risks is viewed as a form of complaining. In this setting a person reporting a risk is viewed as a troublemaker and reaction to the risk is directed at the person rather than at the risk itself. People generally become wary of freely communicating risks under these circumstances and then begin to selectively present the risk information they decide to share to avoid confrontation with team members. Teams creating a positive risk management environment by actively rewarding team members who surface risks will be more successful at identifying and addressing risks earlier than those teams operating in a negative risk environment.

To achieve the goal of maximizing the positive gains for a project, the team must be willing to *take* risks. This requires viewing risks and uncertainty as a means to create the right opportunity for the team to achieve success.

Continuous Assessment

Many information technology professionals misperceive risk management as, at best, a necessary but boring task to be carried out at the beginning of a project or only at the introduction of a new process.

Continuing changes in project and operating environments require project teams to regularly re-assess the status of known risks and to re-evaluate or update the plans to prevent or respond to problems associated with these risks. Projects teams should also be constantly looking for the emergence of new project risks. Risk management activities should be integrated into the overall project life cycle in such a way as to provide appropriate updating of the risk control plans and activities without creating a separate reporting and tracking infrastructure.

Maintain Open Communications

Although risks are generally known by some team members, this information is often poorly communicated. It is often easy to communicate information about risks down the organizational hierarchy, but difficult to pass information about risks up the hierarchy. At every level, people want to know about the risks from lower levels but are wary of upwardly communicating this information. Restricted information flow regarding risks is a potent contributor to project risk because it forces decision making about those risks with even less information. Within the hierarchical organization, managers need to encourage and exhibit open communications about risk and ensure that risks and risk plans are well understood by everyone.

Specify, then Manage

Risk management is concerned with decision making in the face of uncertainty. Generic statements of risk leave much of the uncertainty in place and encourage different interpretations of the risk. Clear statements of risk aid the team in:

- Ensuring that all team members have the same understanding of the risk.
- Understanding the cause or causes of the risk and the relationship to the problems that may arise.
- Providing a basis for quantitative, formal analysis and planning efforts.
- Building confidence by stakeholders and sponsors in the team's ability to manage the risk.

MSF advocates that risk management planning be undertaken with attention to specific information to minimize execution errors in the risk plan that render preventative efforts ineffective or interfere with recovery and corrective efforts.

Don't Judge a Situation Simply by the Number of Risks

Although team members and key stakeholders often perceive risk items as negative, it is important not to judge a project or operational process simply on the number of communicated risks. Risk, after all, is the possibility, not the certainty of a loss or suboptimal outcome. The MSF Risk Management Process advocates the use of a structured risk identification and analysis process to provide decision makers with not only information on the presence of risks but the importance of those risks as well.

Risk Management Planning

During the envisioning and planning phases of the MSF process model, the team should develop and document how they plan to implement the risk management process within the context of the project. Questions to be answered with this plan include:

- What are the assumptions and constraints for risk management?
- How will the risk management process be implemented?
- What are the steps in the process?
- What are the activities, roles, responsibilities, and deliverables for each step?
- Who will perform risk activities?
- What are the skill requirements?
- Is there any additional training?
- How does risk management at the project relate to enterprise level efforts?
- What kinds of tools or methods will be used?
- What definitions are used to classify and estimate risk?
- How will risks be prioritized?
- How will contingency and risk plans be created and executed?
- How will risk control activities be integrated into the overall project plan?
- What activities will team members be doing to manage risk?
- How will status be communicated among the team and project stakeholders?
- How will progress be monitored?
- What kind of infrastructure will be used (databases, tools, repositories) to support the risk management process?
- What are the risks of risk management?
- What resources are available for risk management?
- What are the critical dates in the schedule for implementing risk management?
- Who is the sponsor and who are the stakeholders?

Risk management planning activities should not be viewed in isolation from the standard project planning and scheduling activities, just as risk management tasks should not be viewed as being “in addition” to the tasks team members perform to complete a project. Because risks are inherent in all phases of all projects from start to finish, resources should be allocated and scheduled to actively manage risks. Risk management planning that is carried out by the team during the envisioning and planning phases of the MSF Process Model,[8] and the risk plan that documents those plans, should contribute defined action items assigned to specific team members within the work breakdown structure. These action items should appear on the project plan and master project schedule.

Risk Management Process

Overview of the MSF Risk Management Process

The MSF Risk Management Discipline advocates proactive risk management, continuous risk assessment, and integration into decision-making throughout the project or operational life cycle. Risks are continuously assessed, monitored, and actively managed until they are either resolved or turn into problems to be handled. The MSF Risk Management Process depicted in Figure 1 defines six logical steps through which the team manages current risks, plans and executes risk management strategies, and captures knowledge for the enterprise.

Figure 1 – MSF Risk Management Process

The six steps in the MSF Risk Management Process are:

- Identification
- Analysis and Prioritization
- Planning and Scheduling
- Tracking and Reporting
- Control
- Learning

Risk Identification allows individuals to surface risks so that the team becomes aware of a potential problem. As the input to the risk management process, risk identification should be undertaken as early as possible and repeated frequently throughout the project life cycle.

Risk Analysis transforms the estimates or data about specific project risks that developed during risk identification into a form that the team can use to make decisions around prioritization. *Risk Prioritization* enables the team to commit project resources to manage the most important risks.

Risk Planning takes the information obtained from risk analysis and uses it to formulate strategies, plans, and actions. *Risk Scheduling* ensures that these plans are approved and then incorporated into the standard day-to-day project management process and infrastructure to ensure that risk management is carried out as part of the day-to-day activities of the team. Risk scheduling explicitly connects risk planning with project planning.

Risk Tracking monitors the status of specific risks and the progress in their respective action plans. Risk tracking also includes monitoring the probability, impact, exposure, and other measures of risk for changes that could alter priority or risk plans and project features, resources, or schedule. Risk tracking enables visibility of the risk management process within the project from the perspective of risk levels as opposed to the task completion perspective of the standard operational project management process. *Risk Reporting* ensures that the team, sponsor, and other stakeholders are aware of the status of project risks and the plans to manage them.

Risk Control is the process of executing risk action plans and their associated status reporting. Risk control also includes initiation of project change control requests when changes in risk status or risk plans could result in changes in project features, resources or schedule.

Risk Learning formalizes the lessons learned and relevant project artifacts and tools and captures that knowledge in reusable form for reuse within the team and by the enterprise.

Note that these steps are logical steps and that they do not need to be followed in strict chronologic order for any given risk. Teams will often cycle iteratively through the identification-analysis-planning steps as they develop experience on the project for a class of risks and only periodically visit the learning step for capturing knowledge for the enterprise.

It should not be inferred from the diagram that all project risks pass through this sequence of steps in lock-step. Rather, the MSF Risk Management Discipline advocates that each project define during the project planning phase of the MSF process model when and how the risk management process will be initiated and under what circumstances transitions between the steps should occur for individual or groups of risks.

Identifying Risks

Introduction

Risk identification is the initial step in the MSF Risk Management Process. Risks must be identified and stated clearly and unequivocally so that the team can come to consensus and move on to analysis and planning. During risk identification, the team focus should be deliberately expansive. Attention should be given to learning activity and directed toward seeking gaps in knowledge about the project and its environment that may adversely affect the project or limit its success. Figure 2 depicts graphically the inputs, outputs, and activities for the risk identification step.

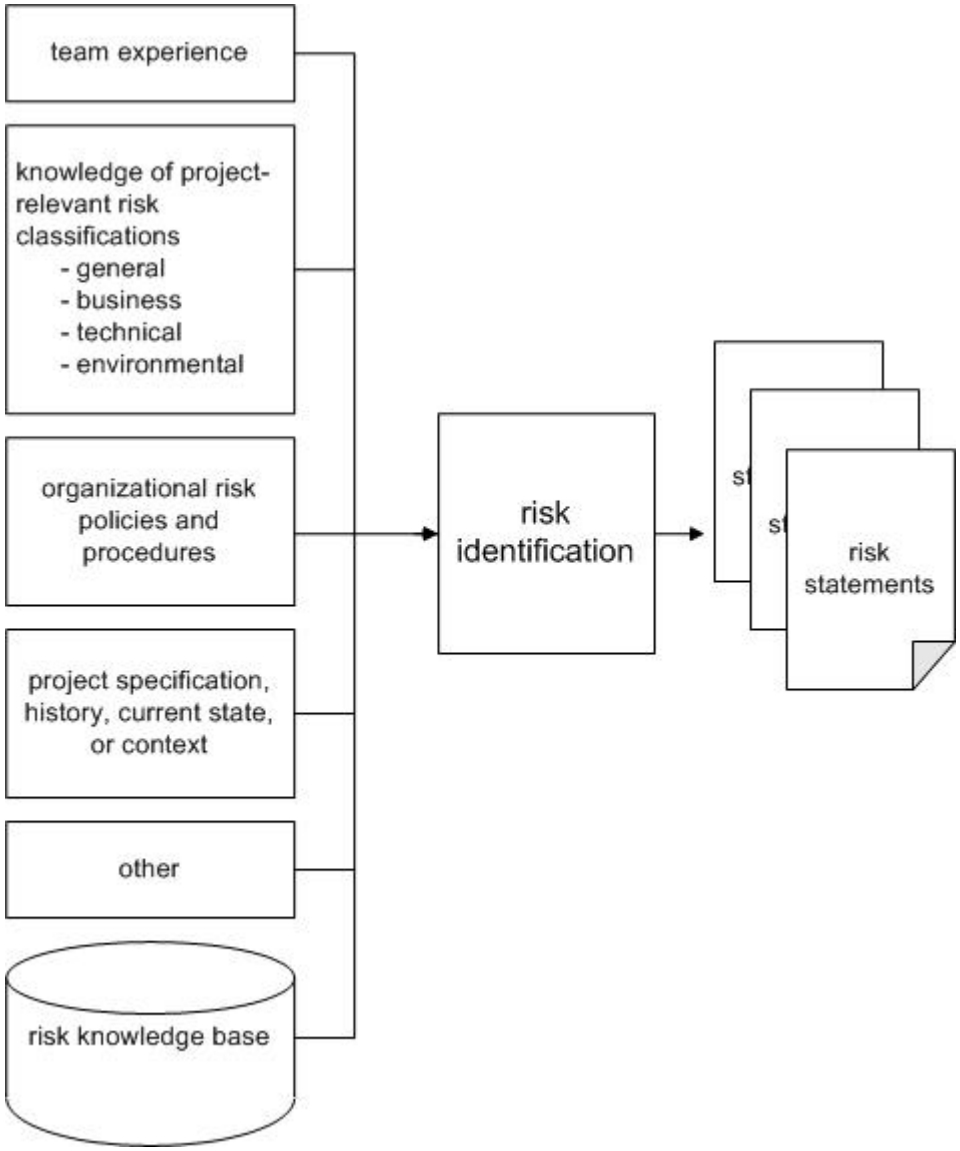

Figure 2 – Risk Identification

Goals

The goal of the risk identification step is for the team to create a list of the risks that they face. This list should be *comprehensive*, covering all areas of the project.

Inputs

The inputs to the risk identification step are the available knowledge of general and project specific risk in relevant business, technical, organizational, and environmental areas. Additional considerations are the experience of the team, the current organizational approach toward risk in the forms of policies, guidelines, templates, and so forth, and information about the project as it is known at that time, including history and current state. The team may choose to draw upon other inputs—anything that the team considers relevant to risk identification should be considered. At the start of a project, it is useful to use group brainstorming, facilitated sessions, or even formal workshops to collect information on project team and stakeholder perceptions on risks and opportunities. Industry classification schemes such as the SEI Software risk taxonomy,[9] project checklists,[10] previous project summary reports, and other published industry sources and guides may also be helpful in assisting the team in identifying relevant project risks.

Risk Identification Activities

During risk identification, the team seeks to create an unambiguous statement or list of risks articulating the risks that they face. At the start of the project it is easy to organize a workshop or brainstorming session to identify the risks associated with a new situation. Unfortunately many organizations regard this as a one-time activity, and never repeat the activity during the project or operations life cycle. MSF Risk Management Discipline emphasizes that risk identification should be undertaken at periodic intervals during a project. Risk identification can be schedule-driven (for example, daily, weekly, or monthly), milestone-driven (associated with a planned milestone in the project plan), or event-triggered (forced by significant disruptive events in the business, technology, organizational or environmental settings). Risk identification activities should be undertaken at intervals and with scope determined by each project team. For example, a team may complete a global risk identification session together at major milestones of a large development project, but may choose in addition to have individual feature teams or even individual developers repeat risk identification for their areas of responsibility at interim milestones or even on a weekly scheduled basis.

During the initial risk identification step in a project, interaction between team members and stakeholders is very important as it is a powerful way to expose assumptions and differing viewpoints. For this reason, MSF Risk Management Discipline advocates involvement of as wide a group of interests, skills, and backgrounds from the team as is possible during risk identification.

Risk identification also may also involve research by the team or involvement of subject matter experts to learn more about the risks within the project domain.

Structured Approach

MSF advocates the use of a structured approach toward risk management where possible. For software development and deployment projects, use of risk classification during the risk identification step is a helpful way to provide a consistent, reproducible, measurable approach. Risk classification provides a basis for standardized risk terminology needed for reporting and tracking and is critical in creating and maintaining enterprise or industry risk knowledge bases. Within the risk identification step, risk classification lists help the team be comprehensive in their thinking about project risk by providing a ready-made, list of project areas to consider from a risk perspective that is derived from previous similar projects or industry experience. Risk statement formulation is the main technique used within MSF for evaluating a specific project and for guiding prioritization and development of specific risk plans.

Risk classification

Risk classifications, or risk categories, sometimes called risk taxonomies, serve multiple purposes for a project team. During risk identification they can be used to stimulate thinking about risks arising within different areas of the project. During brainstorming risk classifications can also ease the complexities of working with large numbers of risks by providing a convenient way for grouping similar risks together. Risk classifications also may be used to provide a common terminology for the team to use to monitor and report risk status throughout the project. Finally, risk classifications are critical for establishing working industry and enterprise risk knowledge bases because they provide the basis for indexing new contributions and searching and retrieving existing work. The following table illustrates a high-level classification for sources of project risk.

People
Customers
End-users
Sponsors
Stakeholders
Personnel
Organization
Skills
Politics
Morale
Process
Mission and goals
Decision making
Project characteristics
Budget, cost, schedule
Requirements
Design
Building
Testing
Technology
Security
Development and test environment
Tools
Deployment
Support
Operational environment
Availability
Environmental
Legal
Regulatory
Competition
Economic
Technology
Business

There are many taxonomies or classifications for general software development project risk. Well-known and frequently-cited classifications that describe the sources of software development project risk include Barry Boehm,[11] Caper Jones,[12] and the SEI Software Risk Taxonomy.[13]

Lists of risk areas covering limited project areas in greater detail are also available. Schedule risk is a common area for project teams and a comprehensive, highly detailed list for assisting software development project teams with risk identification around schedules has been compiled by Steve McConnell.[14]

Different kinds of projects (infrastructure or packaged application deployment), projects carried out with specialized technology domains (such as security, embedded systems, safety critical, EDI), vertical industries (healthcare, manufacturing, and so on.) or product-specific projects may carry well-known project risks unique to that area. Within the area of information security, risks concerning information theft, loss, or corruption as a result of deliberate acts or accidents are often referred to as threats.[15],[16] Projects in these areas will benefit from the review of alternative risk (threat) classifications or extensions to the well-known general purpose risk classifications to ensure breadth of thinking on the part of the project team during the risk identification step.

Other sources for project risk information include industry project risk databases such as the Software Engineering Information Repository (SEIR)[17] or internal enterprise risk knowledge bases.

Risk Statements

A risk statement is a natural language expression expressing a causal relationship between a real, existing project state of affairs or attribute, and a potential, unrealized second project event, state of affairs or attribute. The first part of the risk statement is called the *condition* and it provides the description of an existing project state of affairs or attribute that the team feels may result causally in a project loss or reduction in gain. The second part of the risk statement is a second natural language statement called the *consequence* that describes the undesirable project attribute or state of affairs. The two statement are linked by a term such as “therefore” or “and as a result” that implies an uncertain (in other words, less than 100%) but causal relationship. This is depicted schematically along with an example in figure 3.

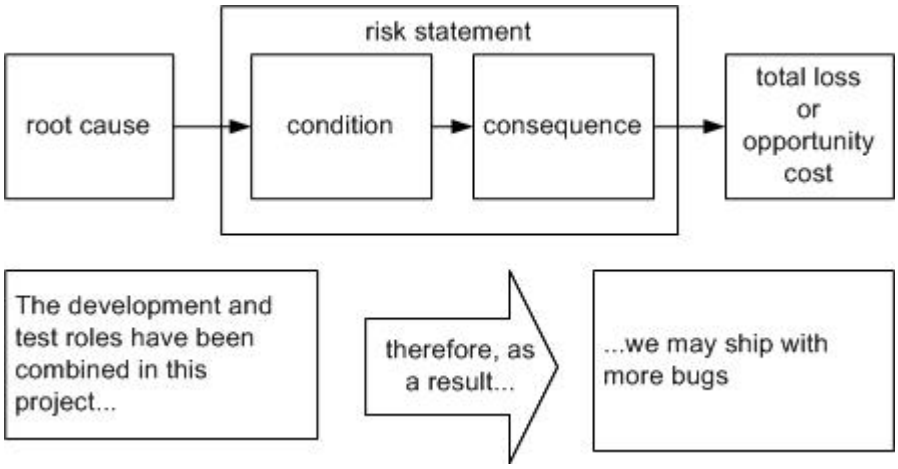

Figure 3 – Risk Statement

The two-part formulation process for risk statements has the advantage of coupling the risk *consequences* with observable (and potentially controllable) risk *conditions* within the project early in the risk identification stage. Use of alternative approaches where the team focuses only on identification of risk conditions within the project during the risk identification stage usually requires that the team backup to recall the risk condition later in on in the risk management process when they develop management strategies.

Note that risk statements are not "if-then" statements, but rather statements of fact exploring the possible but unrealized consequences. During the analysis and planning steps considering hypothetical "if-then" statements may be helpful in weighing alternatives and formulating plans using decision trees. However, during risk identification, the goal is to identify as many risks as possible deferring what-if analysis for the planning phase. Early in the project there should be an abundance of risk statements with conditions that describe the team's lack of knowledge, such as "we do not yet know about X, therefore… ."

When formulating a risk statement, the team should consider both the cause of the potential, unrealized less desirable outcome as well as the outcome itself. The risk statement includes the observed state of affairs (condition) within the project as well as the observable state of affairs that might occur (consequence). As part of a thorough risk analysis, team members should look for similarities and natural groupings of the conditions of project risk statements and backtrack up the causal chain for each condition seeking a common underlying root cause.[18] It is also valuable to follow the causal chain downstream from the condition—consequence pair in the risk statement to examine effects on the organization and environment outside the project to gain a better appreciation for the total losses or missed opportunities associated with a specific project condition.[19]

During risk identification it is not uncommon for the team to identify multiple consequences for the same condition. Sometimes a risk consequence identified in one area of the project may become a risk condition in another. These situations should be recorded by the team so that appropriate decisions can be made during risk analysis and planning to take into account causal dependencies and interactions among the risks. Depending on the relationships among risks, closing one risk may close a whole group of dependent risks and change the overall risk profile for the project. Documenting these relationships early during the risk identification stage can provide useful information for guiding risk planning that is flexible, comprehensive, and which uses available project resources efficiently by addressing root or predecessor causes. The benefits of capturing such additional information at the identification step should be balanced against rapidly moving through the subsequent analysis and prioritization and then re-examining the dependencies and root causes during the planning phase for the most important risks.

Outputs

The minimum output from the risk identification activities is a clear, unambiguous, consensus statement of the risks being faced by the team, recorded as a *risk list*. If the risk *condition-consequence* approach is used as described within the publications from the SEI[20], NASA[21] and earlier versions of MSF[22], [23], then the output will be a collection of risk statements articulating the risks that the project team has identified within the project. The risk list in tabular form is the main input for the next stage of the Risk management process—analysis. The risk identification step frequently generates a large amount of other useful information, including the identification of root causes and downstream effects, affected parties, owner, and so forth.

MSF Risk Management Discipline recommends that a tabular record of the risk statements and the root cause and downstream effect information developed by the team should be created. Additional information for classifying the risks (by project area or attribute) may also be helpful when using project risk information to build or use an enterprise risk knowledge base when a well-defined taxonomy exists. Other helpful information may be recorded in the risk list to define the *context* of the risk to assist other members of the team, external reviewers or stakeholders in understanding the intent of the team in surfacing a risk[24],[25], [26]. Risk context information that some project teams may choose to record during risk identification to capture team intent includes:

- Conditions
- Constraints
- Circumstances
- Assumptions
- Contributing factors
- Dependencies among risks
- Related issues
- Business asset owner
- Team concerns

The tabular risk list (with or without conditions, root causes, downstream effects or context information) will become the master risk list used during the subsequent risk management process steps. An example of a new master risk list is depicted in the following table.

Root Cause	Condition	Consequence	Downstream effect
Inadequate staffing	The roles of development and testing have been combined	We may ship with more bugs	Reduced customer satisfaction
Technology change	Our developers are working with a new programming language	Development time will be longer	We get to the market later and lose market share to competitors
Organization	the development team is divided between London and Los Angeles	Communication among the team will be difficult	Delays in product shipment with additional rework

Analyzing and Prioritizing Risks

Introduction

Risk analysis and prioritization is the second step in the MSF Risk Management process. Risk analysis involves conversion of risk data into a form that facilitates decision-making. Risk prioritization ensures that the team members address the most important project risks first.

During this step, the team examines the list of risk items produced in the risk identification step and prioritizes them for action, recording this order in the master risk list.

From the master risk list, the team can determine a list of “top risks” for which they will commit resources for planning and executing a specific strategy. The team can also identify which risks, if any, are of such low priority for action that they may be dropped from the list. As the project moves toward completion and as project circumstances change, risk identification and risk analysis will be repeated and changes made to the master risk list. New risks may appear and old risks that no longer carry a sufficiently high priority may be removed or “deactivated.” The inputs and outputs to this step are depicted in Figure 4.

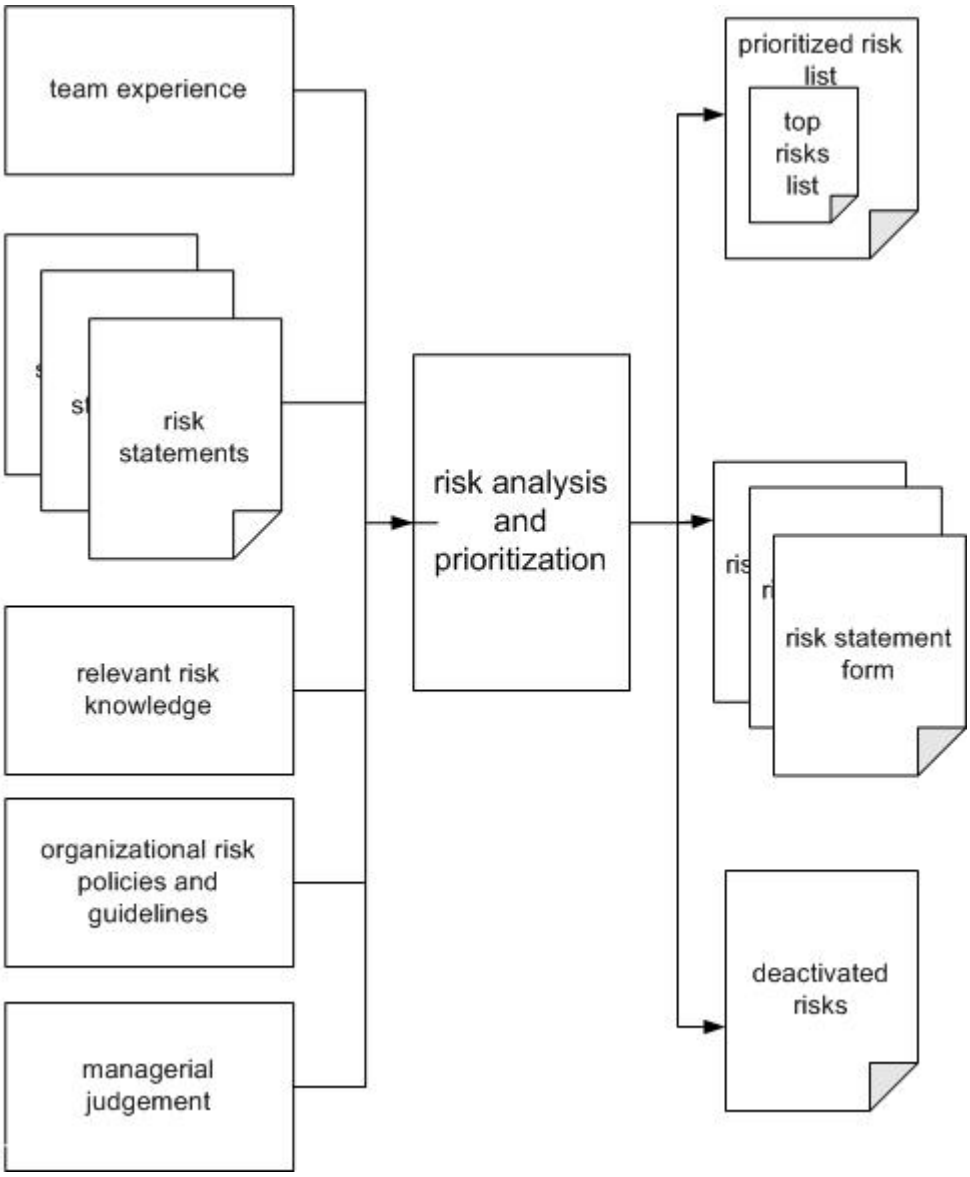

Figure 4 – Risk Analysis and Prioritization

Goal

The chief goal of the risk analysis step is to prioritize the items on the risk list and determine which of these risks warrant commitment of resources for planning.

Inputs

During the risk analysis step the team will draw upon its own experience and information derived from other relevant sources regarding the risks statements produced during risk identification. Relevant information to assist the transformation of the raw risk statements into a prioritized master risk list may be obtained from the organization's risk policies and guidelines, industry risk databases, simulations, analytic models, business unit managers, and domain experts among others.

Risk Analysis Activities

Many qualitative and quantitative techniques exist for accomplishing prioritization of a risk list. One easy-to-use technique for risk analysis is to use consensus team estimates of two widely accepted components of risk, probability, and impact. These quantities can then be multiplied together to calculate a single metric called risk exposure.

Risk Probability

Risk probability is a measure of the likelihood that the state of affairs described in the risk consequence portion of the risk statement will actually occur. Using a numerical value for risk probability is desirable for ranking risks. Risk probability must be greater than zero, or the risk does not pose a threat. Likewise, the probability must be less than 100 percent or the risk is a certainty—in other words, it is a known problem. Probabilities are notoriously difficult for individuals to estimate and apply, although industry or enterprise risk databases may be helpful in providing known probability estimates based on samples of large numbers of projects. Most project teams, however, can verbalize their experience, interpret industry reports, and provide a spectrum of natural language terms that map back to numeric probability ranges. This may be as simple as mapping "low-medium-high" to discrete probability values (17%, 50%, 84%) or as complex as mapping different natural language terms, such as "highly unlikely," "improbable," "likely," "almost certainly," and so on. expressing uncertainty against probabilities. The following table demonstrates an example of a three-value division for probabilities. The next table demonstrates a seven-value division for probabilities.

Probability range	Probability value used for calculations	Natural language expression	Numeric score
1% through 33%	17%	Low	1
34% through 67%	50%	Medium	2
68% through 99%	84%	High	3

Probability range	Probability value used for calculations	Natural language expression	Numeric score
1% through 14%	7%	Extremely unlikely	1
15% through 28%	21%	Low	2
28% through 42%	35%	Probably not	3

Probability range	Probability value used for calculations	Natural language expression	Numeric score
43% through 57%	50%	50-50	4
58% through 72%	65%	Probably	5
73% through 86%	79%	High likelihood	6
87% through 99%	93%	Almost certainly	7

Note that the probability value used for calculation represents the midpoint of a range. With the aid of these mapping tables, an alternative method for quantifying probability is to map the probability range or natural language expression agreed upon by the team to a numeric score. When using a numeric score to represent risk, it is necessary to use the same numeric score for all risks for the prioritization process to work.

No matter what technique is used for quantifying uncertainty, the team will also need to develop an approach for deriving a single value for risk probability that represents their consensus view regarding each risk.

Risk Impact

Risk impact is an estimate of the severity of adverse effects, or the magnitude of a loss, or the potential opportunity cost should a risk be realized within a project. It should be a direct measure of the risk consequence as defined in the risk statement. It can either be measured in financial terms or with a subjective measurement scale. If all risk impacts can be expressed in financial terms, use of financial value to quantify the magnitude of loss or opportunity cost has the advantage of being familiar to business sponsors. The financial impact might be long-term costs in operations and support, loss of market share, short-term costs in additional work, or opportunity cost.

In other situations a subjective scale from 1 to 5 or 1 to 10 is more appropriate for measuring impact. As long as all risks within a master risk list use the same units of measurement, simple prioritization techniques will work. It is helpful to create translation tables relating specific units such as time or money into values that can be compared to the subjective units used elsewhere in the analysis, as illustrated in the following table. This approach provides a highly adaptable metric for comparing the impacts of different risks across multiple projects at an enterprise level. This particular map is a logarithmic transformation where the score roughly equal to the $\log_{10}(\$loss)-1$. High values indicate serious loss. Medium values show partial loss or reduced effectiveness. Low values indicate small or trivial losses.

Score	Monetary Loss
1	Under $100
2	$100-$1000
3	$1000-$10,000
4	$10,000-$100,000
5	$100,000-$1,000,000
6	$1,000,000-$10 million
7	$10 million-$100 million
8	$100 million - $1 billion
9	$1 billion - $10 billion
10	Over $10 billion

When monetary losses cannot be easily calculated the team may choose to develop alternative scoring scales for impact that capture the appropriate project areas. Hall (1998) provides the example[27] in the next table.

Criterion	Cost overrun	Schedule	Technical
Low	Less than 1%	Slip 1 week	Slight effect on performance
Medium	Less than 5%	Slip 2 weeks	Moderate effect on performance
High	Less than 10%	Slip 1 month	Severe effect on performance
Critical	10% or more	Slip more than 1 month	Mission cannot be accomplished

The scoring system for estimating impact should reflect the team and organization's values and policies. A $10,000 monetary loss which is tolerable for one team or organization may be unacceptable for another. Use of a catastrophic impact scored where an artificially high value such as 100 is assigned will ensure that a risk with even a very low probability will rise to the top of the risk list and remain there.

Risk Exposure

Risk exposure measures the overall threat of the risk, combining information expressing the likelihood of actual loss with information expressing the magnitude of the potential loss into a single numeric estimate. The team can then use the magnitude of risk exposure to rank risks. In the simplest form of quantitative risk analysis, risk exposure is calculated by multiplying risk probability and impact.

When scores are used to quantify probability and impact, it is sometimes convenient to create a matrix that considers the possible combinations of scores and assigns them to low risk, medium risk, and high risk categories. For the use of tripartite probability score where 1 is low and 3 is high, the possible results may be expressed in the form of a table where each cell is a possible value for risk exposure. In this arrangement it is easy to classify risks as low, medium, and high depending on their position within the diagonal bands of increasing score.

Probability impact	Low = 1	Medium = 2	High = 3
High = 3	3	6	9
Medium = 2	2	4	6
Low = 1	1	2	3

Low exposure = 1 or 2 Medium exposure = 3 or 4 High exposure = 6 or 9

The advantage of this tabular format is that it allows risks levels to be included within status reports for sponsors and stakeholders using colors (red for the high risk zone in the upper right corner, green for low risk in the lower left corner, and yellow for medium levels of risk along the diagonal) and easy-to-understand, yet well-defined terminology (“high risk” is easier to comprehend than “high exposure”).

Additional Quantitative Techniques

Since the goal of risk analysis is to prioritize the risks on the risk list and to drive decision-making regarding commitment of project resources toward risk control, it should be noted that each project team should select a method for prioritizing risks that is appropriate to the project, the team, the stakeholders, and the risk management infrastructure (tools and processes). Some projects may benefit from use of weighted multi-attribute techniques to factor in other components that the team wishes to consider in the ranking process such as required timeframe, magnitude of potential opportunity gain, or reliability of probability estimates and physical or information asset valuation. An example of a weighted prioritization matrix that factors in not only probability and impact, but critical time window and cost to implement an effective control is shown in the following table, where the formula for the ranking value is calculated using the formula:

Ranking value = 0.5(probability x impact) – 0.2(when needed) + 0.3 (control cost x probability control will work).

Ranking value	Probability	Impact (thousands of dollars)	When needed (weeks)	Cost to implement (thousands of dollars)	Likelihood of control working
125.025	0.5	500	1	2	0.5
83.596	0.84	200	4	4	0.33
37.64	0.33	200	2	20	0.84
4.9816	0.33	30	4	3	0.84

This method allows a team to factor in risk exposure, schedule criticality (when a risk control or mitigation plan must be completed to be effective), and incorporate the cost and efficacy of the plan into the decision-making process. This general approach enables a team to rank risks in terms of the contribution toward any goals that they have set for the project and provides a foundation for evaluating risks both from the perspective of losses (impact) and from opportunities (positive gains).

Selecting the "right" risk analysis method or combination of methods depends on making the right trade-off decision between expending effort on risk analysis or making an incorrect or indefensible (to stakeholders) prioritization choice. Risk analysis should be undertaken to support prioritization that drives decision making, and should never become analysis for the sake of analysis. The results from quantitative or semi-quantitative approaches to risk prioritization should be evaluated within the context of business goals, opportunities, and sound management practices and should not be considered an automated form of decision making by itself.

Outputs

Risk analysis provides the team with a prioritized risk list to guide the team in risk planning activities. Within MSF Risk Management Discipline, this is called the master Risk list. Detailed risk information including project condition, context, root cause, and the metrics used for prioritization (probability, impact, exposure) are often recorded for each risk in the risk statement form.

Master Risk List

MSF Risk Discipline refers to the list of risks as the master risk list. In tabular form, the master risk list identifies the project condition causing the risk, the potential adverse effect (consequence), and the criterion or information used for ranking, such as probability, impact, and exposure. When sorted by the ranking criterion level (high-to-low), the master risk list provides a basis for prioritization in the planning process. An example master risk list using the two-factor (probability and impact) estimate approach is shown in the following table.

Priority	Condition	Consequence	Probability	Impact	Exposure
1	Long project schedule	Loss of funding at end of year	80%	3	2.4
2	No coding standards for new programming language	Ship with more bugs	45%	2	0.9
3	No written requirements specification	Some product features will not be implemented	30%	2	0.6

Low impact = 1, medium impact = 2, high impact = 3

Exposure = Probability x Impact

The master risk list is the compilation of all risk assessment information at an individual project list level of detail. It is a living document that forms the basis for the ongoing risk management process and should be kept up-to-date throughout the cycle of risk analysis, planning, and monitoring.

The master risk list is the fundamental document for supporting active or proactive risk management. It enables team decision making by providing a basis for:

- Prioritizing effort
- Identifying critical actions
- Highlighting dependencies

A list of items maintained in the master risk list is included in the next table. The method that is used to calculate the exposure rendered by a risk should be documented carefully in the risk management plan and care taken to ensure that the calculations accurately capture the intentions of the team in weighing the importance of the different factors.

Item	Purpose	Status
Risk Statement	Clearly articulate a risk	Required
Probability	Quantify likelihood of occurrence	Required
Impact	Quantify severity of loss or magnitude of opportunity cost	Required
Ranking criterion	Single measure of importance	Required
Priority (rank)	Prioritize actions	Required
Owner	Ensure follow through on risk action plans	Required
Mitigation Plan	Describe preventative measures	Required
Contingency plan and triggers	Describe corrective measures	Required
Root cause	Guide effective intervention planning	Optional
Downstream effect	Ensure appropriate impact estimates	Optional
Context	Document background information to capture intent of team in surfacing risk	Optional
Time to implementation	Capture importance that risk controls be implemented within a certain timeframe	Optional

Additional Analysis Methods

Some teams may choose to perform additional levels of analysis to clarify their understanding of project risk. Additional techniques that can be performed by the team to provide additional clarification of project risk are discussed in standard project management and risk management textbooks[28, 29]. Techniques such as decision tree analysis, causal analysis, Pareto analysis, simulation, and sensitivity analysis have all been used to provide a richer quantitative understanding of project risk. The decision to use these tools should be based on the value that the team feels that they bring in either driving prioritization or in clarifying the planning process to offset the resource cost.

Risk Statement Forms

When analyzing each individual project risk or during risk planning activities related to a specific risk, it is convenient to view all of the information on that risk in a document, called the risk statement form.

The risk statement form typically contains the fields from the master risk list created during identification and assessment and may be augmented with additional information needed by the team during the risk management process. When risks will be assigned follow-up action by a separate team or by specific individuals, it is sometimes easier to treat it as a separate document from the master risk list.

Information the team should consider when developing a risk statement form is listed in this table.

Item	Purpose
Risk Identifier	The name the team uses to identify a risk uniquely for reporting and tracking purposes.
Risk Source	A broad classification of the underlying area from which the risk originates, used to identify areas where recurrent root causes of risks should be sought.
Risk Condition	A phrase describing the existing condition that might lead to a loss. This forms the first part of a risk statement.
Risk Consequence	A phrase describing the loss that would occur if the risk became certain. This forms the second part of a risk statement.
Risk probability	A probability greater than zero and less than 100 percent that represents the likelihood that the risk condition will actually occur, resulting in a loss.
Risk Impact Classification	A broad classification of the type of impact a risk might produce.
Risk Impact	The magnitude of impact should the risk actually occur. This number could be the dollar value of a loss or simply a number between 1 and 10 that indicates relative magnitude
Risk Exposure	The overall threat of the risk, balancing the likelihood of actual loss with the magnitude of the potential loss. The team uses risk exposure to rate and rank risks. Exposure is calculated by multiplying risk probability and impact
Risk Context	A paragraph containing additional background information that helps to clarify the risk situation.
Related Risks	A list of risk identifiers the team uses to track interdependent risks

Top Risks List

Risk analysis weighs the threat of each risk to help the team decide which risks merit action. Managing risks takes time and effort away from other activities, so it is important for the team to do only what is absolutely necessary to manage them.

A simple but effective technique for monitoring risk is a top risks list of the major risk items. The top risks list is externally visible to all stakeholders and can be included in the critical reporting documents, such as the vision/scope document, project plan, and project status reports.

Typically, a team will identify a limited number of major risks that must be managed (usually 10 or fewer for most projects) and allocate project resources to address them. Even where the team will eventually want to manage more then the top 10 risks, it is often more effective to concentrate effort on a small number of the greatest risks first and then to move to the less critical risks once the first group is under control.

After ranking the risks, the team should focus on a risk management strategy and how to incorporate the risk action plans into the overall plan.

Deactivating Risks

Risks may be deactivated or classified as inactive so that the team can concentrate on those risks that require active management. Classifying a risk as inactive means that the team has decided that it is not worth the effort needed to track that risk. The decision to deactivate a risk is taken during risk analysis.

Some risks are deactivated because their probability is effectively zero and likely to remain so, i.e., they have extremely unlikely conditions. Other risks are deactivated because their impact is below the threshold where it’s worth the effort of planning a mitigation or contingency strategy; it’s simply more cost-effective to suffer the impact if the risk arises. Note that is not advisable to deactivate risks above this impact threshold even if their exposure is low, unless the team is confident that the probability (and hence the exposure) will remain low in all foreseeable circumstances. Also note that deactivating a risk is not the same as resolving one; a deactivated risk might reappear under certain conditions and the team may choose to reclassify the risk as active and initiate risk management activities.

Risk Planning and Scheduling

Introduction

Risk planning and scheduling is the third step in the risk management process. The planning activities carried out by the team translate the prioritized risk list into action plans. Planning involves developing detailed strategies and actions for each of the top risks, prioritizing risk actions, and creating an integrated risk management plan. Scheduling involves the integration of the tasks required to implement the risk action plans into the project schedule by assigning them to individuals and actively tracking their status. This step is depicted schematically in Figure 5.

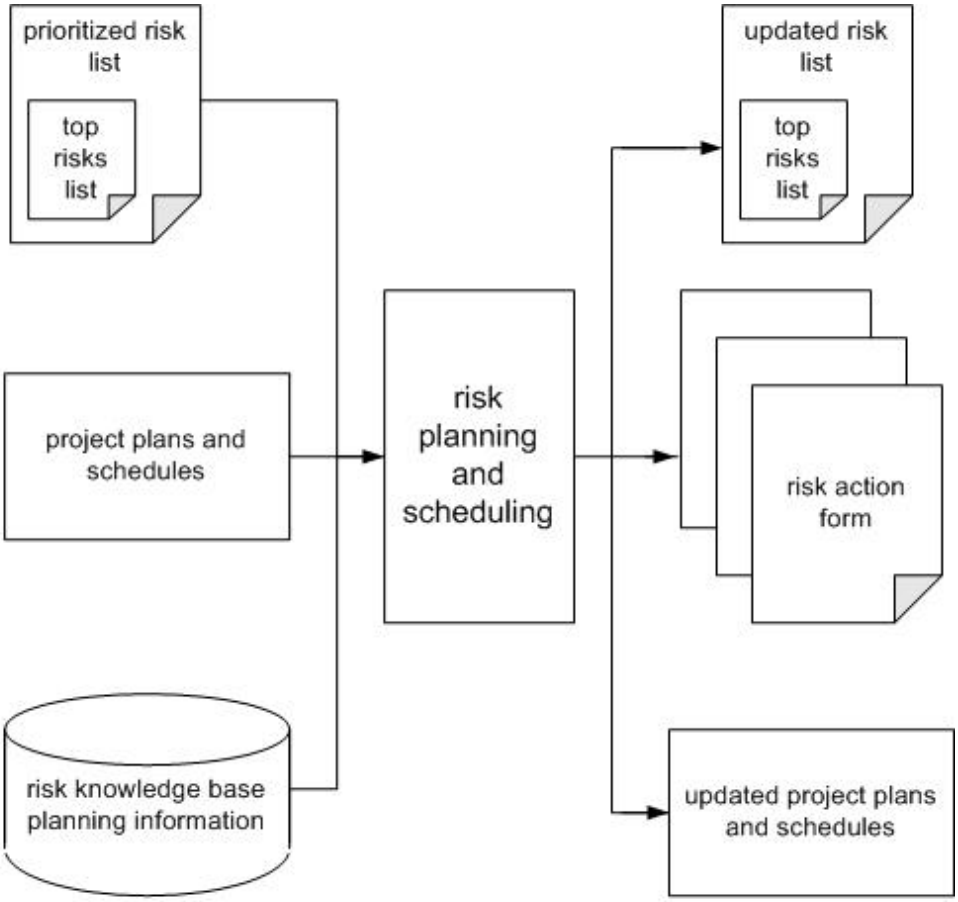

Figure 5 –Risk Planning and Scheduling

The master risk list is updated with additional information for the top risks identified during risk analysis. Sometimes it is convenient to present those parts of the master risk list used during planning as a separate risk action form for use by team members who have been assigned risk action items.

Goals

The main goal of the risk planning and scheduling step is to develop detailed plans for controlling the top risks identified during risk analysis and to integrate them with the standard project management processes to ensure that they are completed.

Inputs

MSF Risk Management Discipline advocates that risk planning be tightly integrated into the standard project planning processes and infrastructure. Inputs to the Risk planning process includes not only the master risk list, top risks list, and information from the risk management knowledge base, but also the project plans and schedules.

Planning Activities

When developing plans for reducing risk exposure:

- Focus on high-exposure risks.
- Address the condition to reduce the probability.
- Look for root causes as opposed to symptoms.
- Address the consequences to minimize the impact.
- Determine the root cause, then look for similar situations in other areas that may arise from the same cause.
- Be aware of dependencies and interactions among risks.

Several approaches are possible to reduce risk:

- For those risks the team can control, apply the resources needed to reduce the risk.
- For those risks outside the control of the team, find a work-around or transfer (escalate) the risk to individuals that have the authority to intervene.

During risk action planning, the team should consider these six alternatives when formulating risk action plans.

- *Research.* Do we know enough about this risk? Do we need to study the risk further to acquire more information and better determine the characteristics of the risk before we can decide what action to take?
- *Accept.* Can we live with the consequences if the risk were actually to occur? Can we accept the risk and take no further action?
- *Avoid.* Can we avoid the risk by changing the scope?
- *Transfer.* Can we avoid the risk by transferring it to another project, team, organization or individual?
- *Mitigation.* Can the team do anything to reduce the probability or impact of the risk?
- *Contingency.* Can the impact be reduced through a planned reaction?

Research

Much of the risk that is present in projects is related to the uncertainties surrounding incomplete information. Risks that are related to lack of knowledge may often be resolved or managed most effectively by learning more about the domain before proceeding. For example, a team may choose to pursue market research or conduct user focus groups to learn more about user baseline skills or willingness to use a given technology before completing the project plan. If the decision by the team is to perform research, then the risk plan should include an appropriate research proposal including hypotheses to be tested or questions to be answered, staffing, and any needed laboratory equipment.

Accept

Some risks are such that it is simply not feasible to intervene with effective preventative or corrective measures, but the team elects to simply accept the risk in order to realize the opportunity. Acceptance is not a “do-nothing” strategy and the plan should include development of a documented rationale for why the team has elected to accept the risk but not develop mitigation or contingency plans. It is prudent to continue monitoring such risks through the project life cycle in the event that changes occur in probability, impact or the ability to execute preventative or contingency measures related to this risk. These ongoing commitments to monitor or watch a risk should have appropriate resources committed and tracking metrics established within the overall project management process.

Avoid

On occasion, a risk will be identified that can be most easily controlled by changing the scope of the project in such a fashion as to eliminate the risk all together. The risk plan should then include documentation of the rationale for the change, and the project plan should be updated and any needed design change or scope change processes initiated.

Transfer

Sometimes it is possible for a risk to be transferred so that it may be managed by another entity outside of the project. Examples where risk is transferred include:

- Insurance
- Using external consultants with greater expertise
- Purchasing a component instead of building it
- Outsourcing services

Risk transfer does not mean risk elimination. In general a risk transfer strategy will generate risks that still requirement proactive management, but reduce the level of risk to an acceptable level. For instance, using an external consultant may transfer technical risks outside of the team, but may introduce risks in the project management and budget areas.

Mitigation

Risk mitigation planning involves actions and activities performed ahead of time to either prevent a risk from occurring altogether or to reduce the impact or consequences of its occurring to an acceptable level. Risk mitigation differs from risk avoidance because mitigation focuses on prevention and minimization of risk to acceptable levels, whereas risk avoidance changes the scope of a project to remove activities having unacceptable risk.

The main goal of risk mitigation is to reduce the probability of occurrence. For example, using redundant network connections to the Internet reduces the probability of losing access by eliminating the single point of failure.

Not every project risk has a reasonable and cost-effective mitigation strategy. In cases where a mitigation strategy is not available, it is essential to consider effective contingency planning instead.

Contingency Planning

Risk contingency planning involves creation of one or more fallback plans that can be activated in case efforts to prevent the adverse event fail. Contingency plans are necessary for all risks, including those that have mitigation plans. They address what to do if the risk occurs and focus on the consequence and how to minimize its impact. To be effective, the team should make contingency plans well in advance. Often the team can establish trigger values for the contingency plan based on the type of risk or the type of impact that will be encountered.

There are two types of contingency triggers:

- Point-in-time triggers are built around dates, generally the latest date by which something has to happen.
- Threshold triggers rely on things that can be measured or counted.

It is important for the team to agree on contingency triggers and their values with the appropriate managers as early as possible so that there is no delay committing budgets or resources needed to carry out the contingency plan.

Scheduling Activities

Scheduling risk management and control activities does not differ from the standard approach recommended by MSF toward scheduling project activities in general.[30] It is important that the team understand that risk control activities are an expected part of the project and not an additional set of responsibilities to be done on a voluntary basis. All risk activities should be accounted for within the project scheduling and status reporting process.

Outputs

The output from the risk action planning should include specific risk action plans implementing one of the six approaches discussed above at a step-by-step level of detail. The tasks to implement these plans should be integrated into the standard project plans and schedules. This includes adjustments in committed resources, schedule, and feature set, resulting in a set of risk action items specifying individual tasks to be completed by team members. The master risk list should be updated to reflect the additional information included in the mitigation and contingency plans. It is convenient to summarize the risk management plans into a single document.

Risk Action Items

Risk action items are logged in the team's normal project activity-tracking system so that they are regarded as just as important as any other actions.

Like all properly documented actions, they should be associated with a due date for completion and a personnel assignment, so there is no confusion over who is responsible for their completion.

Risk Action Forms

The team should develop additional planning information for each risk in the top risk list to document the mitigation and contingency plans, triggers, and actions in detail. Information the team might consider when developing a risk action form or document includes the following:

- *Risk Identifier*. The name the team uses to identify a risk uniquely for reporting and tracking purposes.
- *Risk Statement*. A natural language statement describing the condition that might lead to a loss and the loss that would occur if the risk were to become certain.
- *Risk Mitigation Strategy*. A paragraph or two of text describing the team strategy for mitigating a specific risk, including any assumptions that have been made.
- *Risk Mitigation Strategy Metrics*. The metrics the team will use to determine whether the planned risk mitigation actions are achieving the desired results.
- *Risk Action Items*. A list of actions the team is taking to implement the strategy for a specific risk, including the due date for completion and the person responsible.
- *Risk Contingency Strategy*. A paragraph or two describing the team strategy in the event that the actions planned to manage the risk don't work. The team would execute the risk contingency strategy if the risk contingency trigger were reached.
- *Contingency Trigger Values*. Contingency triggers are the criteria that teams use to determine when to execute contingency plans.
- *Risk Contingency Strategy Metrics*. The metrics used by the team to determine if the contingency strategy is working.
- *Risk Plan Responsibility*. The team role and individual(s) that hold responsibility for implementing the risk action plan.

Updated Project Schedule and Project Plan

Planning documents related to risk should be integrated into the overall project planning documents and the master project schedule updated with the new tasks generated by the plans.

Risk Tracking and Reporting

Risk tracking is the fourth step in the MSF Risk Management Process. Risk tracking is essential to implementing action plans effectively. It ensures that assigned tasks implementing preventative measures or contingency plans are completed in a timely fashion within project resource constraints. During risk tracking the principal activity performed by the team is monitoring the risk metrics and triggering events to ensure that the planned risk actions are working. Tracking is the monitoring function of the risk action plan. Risk tracking is depicted schematically in Figure 6.

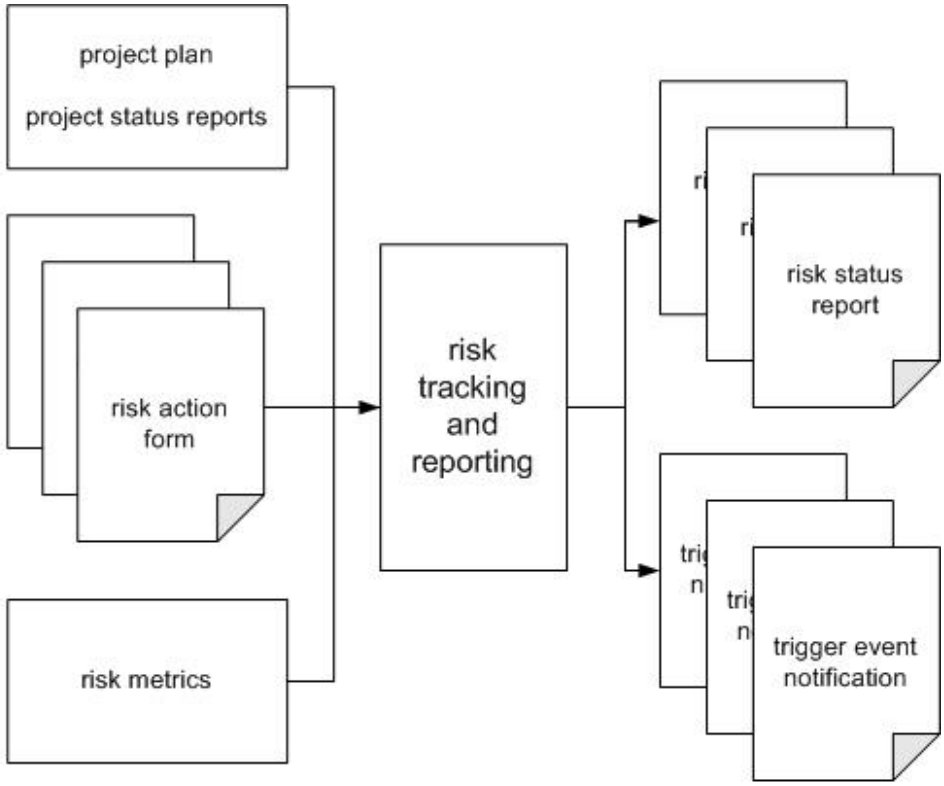

Figure 6 – Risk Tracking and Reporting

Goals

The goals of the risk tracking step are to monitor the status of the risk action plans (progress toward completion of contingency and mitigation plans), to monitor project metrics that have been associated with a contingency plan trigger, and to provide notification to the project team that contingency plan triggers have been exceeded so that a contingency plan can be initiated.

Inputs

The principal inputs to the risk tracking step are:

- The risk action forms that contain the specific mitigation and contingency plans and which specify the project metrics and trigger values to be monitored.
- The relevant project status reports that are used to track progress within the standard project management infrastructure.

Depending on the specific project metrics being tracked by the team, other sources of information such as project tracking databases, source code repositories or check-in systems, or even human resources management systems may provide tracking data for the project team.

Tracking Activities

During the risk tracking step the team executes the actions in the mitigation plan as part of the overall team activity. Progress toward these risk-related action items and relevant changes in the trigger values are captured and used to create the specific risk status reports for each risk.

Examples of project metrics that might be assigned trigger metrics and continuously tracked include:

- Unresolved (open bugs) per module or component.
- Average overtime hours logged per week per developer.
- Number of requirement revisions (changes) per week.

Risk Status Reporting

Risk reporting should operate at two levels. For the team itself, regular risk status reports should consider four possible risk management situations for each risk:

- A risk is resolved, completing the risk action plan.
- Risk actions are consistent with the risk management plan, in which case the risk plan actions continue as planned.
- Some risk actions are at variance to the risk management plan, in which case corrective measures should be defined and implemented.
- The situation has changed significantly with respect to one or more risks and will usually involve re-analyzing the risks or re-planning an activity.

For external reporting to the project stakeholders, the team should report the top risks and then summarize the status of risk management actions. It is also useful to show the previous ranking of risks and the number of times each risk has been in the top risk list. As the project team takes actions to manage risks, the total risk exposure for the project should begin to approach acceptable levels.

Outputs

The purpose of the risk status report is to communicate changes in the status of the risk and report progress for mitigation plans. Information that is useful in the risk status report includes:

- Risk name
- Risk classification (project area)
- Probability, Impact, and Exposure at identification
- Current Probability, Impact, and Exposure
- Risk level (low, medium, high)
- Summary of mitigation and contingency plan(s)
- Status toward completion of mitigation plans (completed actions)
- Readiness of contingency plans
- Trigger values
- Planned actions
- Risk owner

The purpose of an executive or stakeholder risk status report is to communicate the overall risk status of the project. Useful information to include in this report includes:

- Project name
- Risk level by project area
- Risk trend
- Summary of mitigation and contingency plan activity

This report is often included within the standard project status report.

Risk Control

The fifth step in the MSF Risk Management Process is risk control. During this step the team is actively performing activities related to contingency plans because triggers have been reached. This step is depicted in Figure 7.

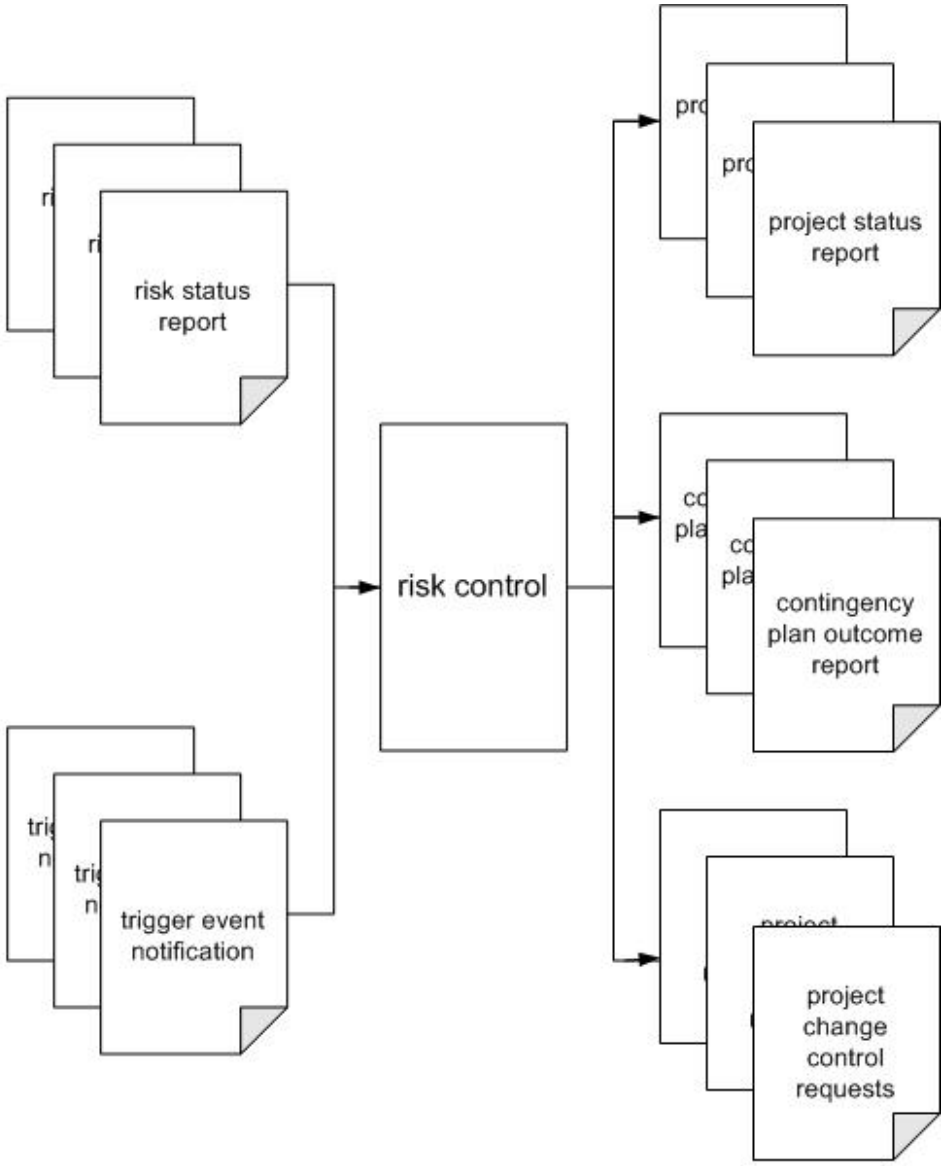

Figure 7 – Risk Control

Corrective actions are initiated based on the information gained from risk tracking. MSF Risk Management Discipline relies on existing standard project management processes and infrastructure to:

- Control risk action plans.
- Correct for variations from plans.
- Respond to triggering events.

The results and lessons learned from execution of contingency plans are then incorporated into a contingency plan status and outcome report so that the information will become part of the project and enterprise risk knowledge base. It is important to capture as much information as is possible about problems when they incur or about a contingency plan when it is invoked to determine the efficacy of such a plan or strategy on risk control.

Goals

The goal of the risk control step is successful execution of the contingency plans that the project team has created for top risks.

Inputs

The inputs to the risk control step are the risk action forms that detail the activities to be carried out by project team members and risk status reports that document the project metric values that indicate that a trigger value has been exceeded.

Control Activities

Risk control activities should utilize the standard project management processes for initiating, monitoring, and assessing progress along a planned course of action. The specific details of the risk plans will vary from project to project, but the general process for task status reporting should be used. It is important to maintain continuous risk identification to detect secondary risks that may appear or be amplified because of the execution of the contingency plan.

Outputs

The output from the risk control step is the standard project status report documenting progress toward the completion of the contingency plan. It is helpful for the project team to also summarize the specific lessons learned (for example, what worked, what did not work) around the contingency plan in the form of a contingency plan outcome summary. Changes in risk status which could require changes in schedule, resources, or project features (for example, execution of a contingency plan) should also result in creation of a change control request in those projects having formal change control processes.

Learning from Risk

Introduction

Learning from risk is the sixth and last step in the MSF Risk Management Process and adds a strategic, enterprise, or organizational perspective to risk management activities. This step is sometime referred to as risk leverage, emphasizing the value that is returned to the organization by increased capabilities and maturing at the team, project, or organizational levels, and improvement of the risk management process. Risk learning should be a continuous activity throughout the MSF Risk Management Process and may begin at any time. It focuses on three key objectives:

- Providing quality assurance on the current risk management activities so that the team can gain regular feedback.
- Capturing lessons learned, especially around risk identification and successful mitigation strategies, for the benefit of other teams; this will contribute to the risk knowledge base.
- Improving the risk management process by capturing feedback from the team.

Risk review meetings provide the forum for learning from risk. They should be held on a regular basis and, like other MSF reviews, they benefit from advance planning, development of a clear, published agenda in advance, participation by all participants, and free, honest, communication in a “blame-free” environment. Figure 8 depicts the learning phase schematically.

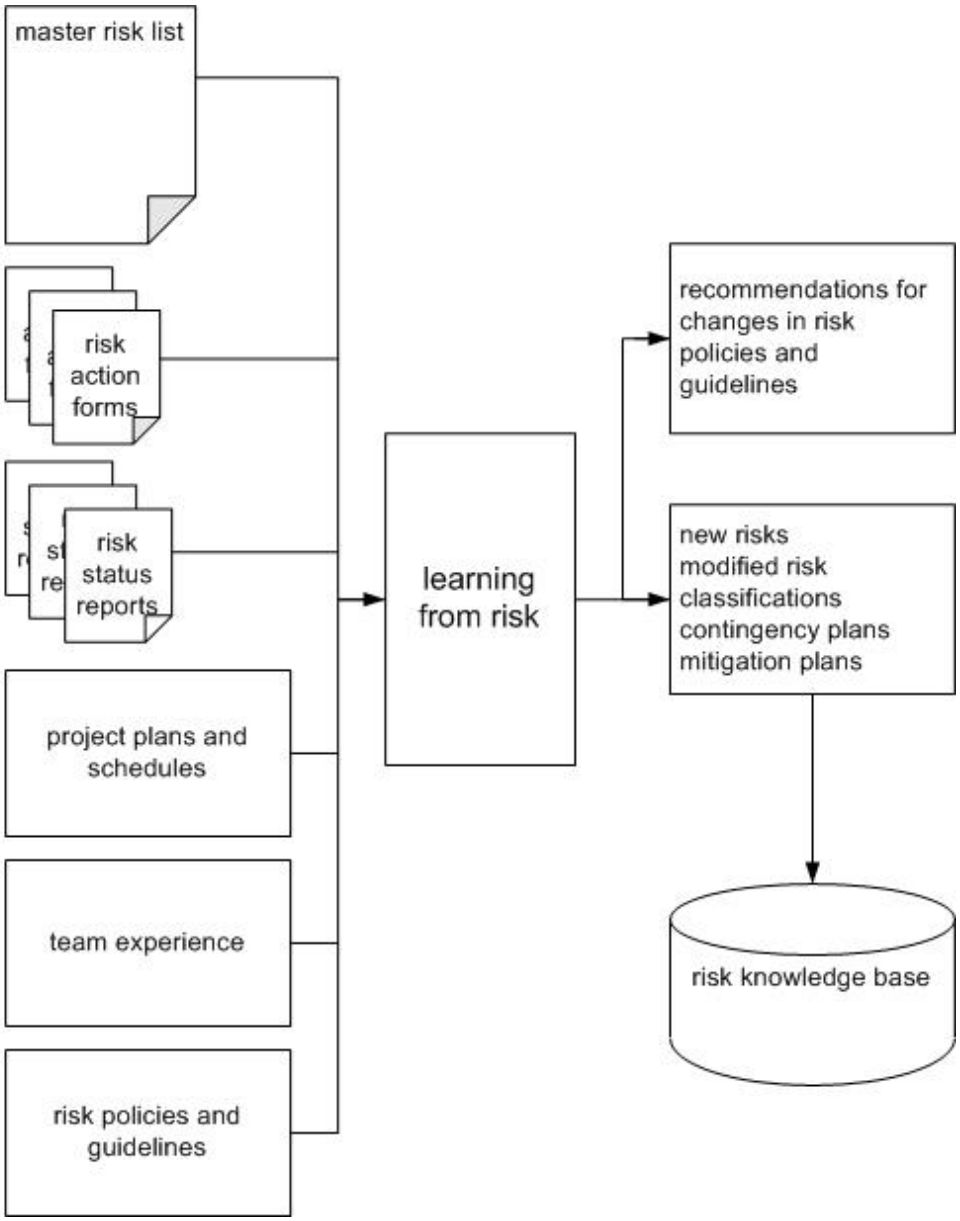

Figure 8 – Learning from Risk

Capturing Learning about Risk

Risk classification definition is a powerful means for ensuring that lessons learned from previous experience are made available to teams performing future risk assessments. Two key aspects of learning are often recorded using risk classifications:

- *New risks.* If a team encounters an issue that had not been identified earlier as a risk, it should review whether any signs (leading indicators) could have helped to predict the risk. It may be that the existing risk lists need to be updated to help future identification of the risk condition. Alternatively, the team might have identified a new project risk which should be added to the existing risk knowledge base.
- *Successful mitigation strategies.* The other key learning point is to capture experiences of strategies that have been used successfully (or even unsuccessfully) to mitigate risks. Use of a standard risk classification provides a meaningful way to group related risks so that teams can easily find details of risk management strategies that have been successful in the past.

Managing Learning from Risks

Organizations using risk management techniques often find that they need to create a structured approach to managing project risk. Conditions to successfully facilitate this requirement include:

- An individual should be given ownership of a specific risk classification area and responsibility for approving changes.
- Risk classifications should balance the need for a comprehensive coverage of risks against complexity and usability. Sometimes creating different risk classifications for different project types can improve usability dramatically.
- A risk knowledge base should be set up to maintain risk classifications, definitions, diagnostic criteria, and scoring systems, and to capture feedback on the team's experience with using them.
- The risk review process should be well managed to ensure all learning is captured. For a project team, reviews may be held at the project closure review, when the results of risk management should be apparent to all.

Context-Specific Risk Classifications

Risk identification can be refined by developing risk classifications for specific repeated project contexts. For example a project delivery organization may develop classifications for different types of project. As more experience is gained on work within a project context, the risks can be made more specific and associated with successful mitigation strategies.

Risk Knowledge Base

The risk knowledge base is a formal or informal mechanism by which an organization captures learning to assist in future risk management. Without some form of knowledge base, an organization may have difficulty adopting a proactive approach to risk management. The risk knowledge base differs from the risk management database which is used to store and track individual risk items, plans, and status during the project.

Developing Maturity in Managing Knowledge about Risk

The risk knowledge base is the key driver of continual improvement in risk management.

At the lowest level of maturity, project and process teams have no form of knowledge base. Each team has to start fresh every time it undertakes risk management. In this environment, the approach to risk management is normally reactive, but may transition to the next higher level of active risk management. However, the team does not manage risks proactively.

The next level of maturity involves an informal knowledge base, using the implicit learning gained by more experienced members of the organization. This is often achieved by implementing a risk board where experienced practitioners can review how each team is performing. This approach encourages active risk management and might lead to limited proactive management through the introduction of policies. An example of a proactive risk management policy is “all projects of more than 20 days need a risk review before approval to proceed.”

The first level of formality in the knowledge base comes through providing a more structured approach to risk identification. The MSF Risk Management Discipline advocates the use of risk classifications for this purpose. With formal capture and indexing of experience, the organization is capable of much more proactive management as the underlying causes of risks start to be identified.

Finally, mature organizations record not only the indicators likely to lead to risk, but also the strategies adopted to manage those risks and their success rate. With this form of knowledge base the identification and planning steps of the risk process can be based on shared experience from many teams and the organization can start to optimize its costs of risk management and return on project investment.

When contemplating implementation of a risk knowledge base, experience has shown that:

- The value of the risk knowledge base increases as more of the work becomes repetitive (such as organizations focusing on similar projects, or for on-going operational processes).
- When an organization is focused on one-of projects, a less complex knowledge base is easier to maintain.

Risk management should not become an automatic process that obviates the need for the team to think about risks. Even in repetitive situations, the business environment, customer expectations, team skills, and technology are always changing. The team, therefore, must assess the appropriate risk management strategies for their specific project situation.

Integrated Risk Management in the Project Lifecycle

The MSF Risk Management Process is closely integrated into the overall project life cycle. Risk assessment can begin during envisioning as the project team and stakeholders begin to frame the project vision and begin setting constraints. With each constraint and assumption that is added to the project, additional risks will begin to emerge. The project team should begin risk identification activities as early in the project as possible. During the risk analysis and planning stages, the needed risk mitigation and contingency plans should be built directly into the project schedule and master plan. Progress of the risk plan should be monitored by the standard project management process.

Although the risk management process will generally start with scheduled initial risk identification and analysis sessions, thereafter the risk planning, tracking, and controlling steps will be completed as different blocks of activity for different risks on the master risk list. Within MSF Risk Discipline, continuous risk management assumes that the project team is “always” simultaneously in the state of risk identification and risk tracking. They will engage in risk control activities when called for by triggering events and the project schedule and plan. However, over the full project life cycle, new risks will emerge and require initiation of additional analysis and planning sessions. There is no requirement to synchronize any one of the risk management steps with any of specific project life cycle milestones. Some teams will initiate risk identification and analysis activity at major milestones as convenient opportunities to reassess the state of the project. It is convenient to summarize learning around risk at the same time.

In general, risk identification and risk tracking are continuous activities. Team members should be constantly looking for risks to the project and surfacing them for the team to consider, as well as tracking continuously the progress against specific risk plans. Analyzing and re-analyzing risks as well as modifying the risk management action plans are more likely to be intermittent activities for the team, sometimes proactively scheduled (perhaps around major milestones), and sometime as a result of a unscheduled project event (discovery of additional risks during tracking and control). Learning is most often a scheduled event occurring around major milestones and certainly at the end of the project.

Over the course of the project the nature of risks being addressed should change as well. Early in the project, business, scope, requirements, and design related risks will dominate. As time progresses, technical risks surrounding implementation become more prominent, and then transition to operational risks. It is helpful to utilize risk checklists or review risk classification lists at each major phase transition within the project life cycle to guide risk identification activity.

Risk Management in the Enterprise

To achieve maximum return on risk management efforts it is important to maintain an enterprise view that treats risk management across the enterprise.

Creating a Risk Management Culture

While few project delivery organizations argue against managing risks in their projects, many find it difficult to fully adopt the discipline associated with a proactive risk management process. Often they might undertake a risk assessment at the start of each project, but fail to maintain the process as the project proceeds.

Two reasons are frequently put forward to explain this approach:

- Pressure of time on the project team.
- Concern that focus on risks will undermine the customer's confidence or present a negative impression.

The root cause for these beliefs is often that managers themselves do not understand the value that risk management delivers to a project. As a result they are reluctant to propose adequate time for risk management (and indeed other project management activities) in the project budget. Conversely, they might sacrifice these activities first if the budget comes under pressure.

It is therefore especially important to ensure that all stakeholders appreciate the importance of managing risks in order to establish a culture where risk management can thrive. The following steps have been found effective in establishing risk management as a consistent discipline:

- Secure management sponsorship.
- Seek advice and mentorship from a risk manager who can bring personal experiences and knowledge of failures.
- Educate all stakeholders about the importance of managing risks and the costs that can be incurred from failure.
- Train a core set of risk managers who can provide role models and mentorship for others; an effective training approach is to combine a workshop on the theory of risk management with real exercises based on a live project.
- Invite all project stakeholders to risk review meetings and ensure that status reports are circulated to them.
- Introduce a recognition scheme for project team members who effectively identify and/or manage risks.
- Ensure that project teams consider risks in project scheduling and making key decisions.
- Seek feedback from stakeholders on the effectiveness of the risk management process and review it regularly to ensure that it is seen to add value.
- Reward team members that surface risks.

Managing a Portfolio of Projects

Project delivery organizations can benefit from introducing a process to manage risks across their portfolio of projects. Typically the benefits include the following:

- Resources and effort can be assigned to projects across the portfolio according to the risks they face.
- Each project's risk manager has an external escalation point to provide a second opinion on the team's assessments.
- Project teams can learn more rapidly from experience elsewhere.
- Quality assurance on the risk management processes is applied within each project.

It should be noted that the portfolio risk review complements the risk assessments that are undertaken by each project team. The review team does not have the project knowledge to identify risks, nor does it have the time available to undertake risk mitigation actions. However, it can contribute to risk analysis and planning.

Since the review group normally contains more experienced managers, its members can often call on that experience to advise the project team on the significance of certain risk, helping the team to prioritize risks. They can also recommend mitigation and contingency strategies that they have seen used effectively in the past.

The following are successful practices that have been applied in portfolio risk management:

- Secure executive support for the portfolio review process. Maintain this by regular reports on findings and lessons learned.
- Schedule the meetings well in advance; ideally make it a recurring, regular appointment on a day when many of the project leads can be expected to be present. Issue invitations to the review board well in advance; good reviewers will have many other commitments.
- Select projects for review carefully. You might expect to review the biggest projects every month, but ensure that a broad cross-section of medium-sized projects is also reviewed.
- Follow a standard agenda for each project, so that project leads know what to expect from the meeting. For example, one practice allowed 20 minutes for presentation of the current risk assessment, followed by 20 minutes discussion of the mitigation and contingency strategies, followed by a 5-minute review of any lessons learned to be shared with other project teams.
- Use standard documents for project status reporting and risk assessment.
- Ensure both documents are updated and distributed to all attendees in advance of the meeting; this will enable you to reduce the time spent in the meeting.
- Encourage project team leads to attend the review, either in person or on the telephone.
- Ensure that the project team gets value from the review. Often this can be achieved by reviewing progress on issues that might not technically be risks, but where the experience of the review board members can assist the project team.
- Avoid attributing any blame for the project situation.
- Allow any project member to request a review on their project.

Summary

MSF Risk Management Discipline advocates the use of proactive, structured risk management for software development and deployment projects. The MSF Risk Management Process consists of six logical steps (identification, analysis, planning, tracking, controlling, and learning) through which a project team should cycle continuously during the project life cycle. The learning step is used to communicate project risk lessons learned and feedback on enterprise-level risk management resources to an enterprise-wide risk knowledge base.

[1] MSF Process Model v. 3.0, 2002 (available at http://www.microsoft.com/msf)

[2] Audrey J. Dorofee, Julie A. Walker, Christopher J Alberts et al, *Continuous Risk Management Guidebook* (Carnegie-Mellon University, 1996).

[3] Ronald P. Higuera, "Team Risk Management: A New Model for Customer-Supplier Relationships", *SEI Technical Report CMU/* SEI-94-SR-5, (Pittsburgh, PA: Software Engineering Institute—Carnegie Mellon University), 1994.

[4] Encarta 2002, Article "Insurance. II. Reasons for Insurance".

[5] Jim McCarthy, *Dynamics of Software Development* (Redmond, Washington: Microsoft Press, 1995), page 99.

[6] The eight principles are 1. expect things to change – stay agile. 2. work toward a shared vision. 3. focus on delivering business value throughout the life cycle. 4. invest in quality. 5. learn from all experiences – good and bad, 6. foster open communication 7. clear accountability, shared responsibility 8. empowered team.

[7] MSF Team Model 3.0 Whitepaper (http://www.microsoft.com/msf).

[8] See MSF 3.0 Process Model Whitepaper for deeper discussion, available at http://www.microsoft.com/msf

[9] Ronald P. Higuera and Yacov Y. Haimes, "Software Risk Management", *SEI Technical Report CMU*/SEI-96-TR-012 ESC-96-012 (Pittsburgh, PA: Software Engineering Institute—Carnegie Mellon University, 1996).

[10] For example, Steve McConnell, *Software Project Survival Guide*, (Redmond, WA: Microsoft Press), 1998.

[11] Barry W. Boehm, *Software Risk Management*, (New York, NY: IEEE Press), 1989.

[12] Capers Jones, *Assessment and Control of Software Risks*. (Englewood, NJ: Prentice-Hall, 1994). ISBN 0-13-741406-4

[13] Ronald P. Higuera and Yacov Y. Haimes, "Software Risk Management*", SEI Technical Report*, 1996.

[14] Steve McConnell, *Rapid Development*, (Redmond, Microsoft Press), 1996, pp 87-91.

[15] Thomas R. Peltier, *Information Security Risk Analysis*, (Boca Raton: Auerbach Publications, 2001).

[16] Donald L Pipkin, *Information Security: Protecting the Global Enterprise*, (Newark, NJ: Prentice Hall, 2000).

[17] http://seir.sei.cmu.edu/

[18] One effective brainstorming technique for root cause identification is called "Five Whys". In this approach, the group should ask the question "why is that?" of the risk condition,, provide an answer, and the repeat the "why is that? – because of …" cycle for up to five times.

[19] This can be accomplished by a variant of the "5-Why" technique where the team cycles through the "so what?..Because then …" question and answer sequence five times.

[20] Audrey J Dorofee, Julie A Walker, Christopher J Alberts, et al., *Continuous Risk Management Guidebook.* (Pittsburgh, PA: Carnegie Mellon University, 1996).

[21] Linda H Rosenberg , Theodore Hammer , Albert Gallo, *Continuous Risk Management at NASA*, 1999 (http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html)

[22] *MSF Risk Management Process* Whitepaper, 2001.

[23] *Principles of Application Development*- Course 593 and Course 1517.

[24] Rosenberg LH, et al., 1999.

[25] Elaine Hall, Managing Risk. *Methods for Software Systems Development, SEI Series in Software Engineering*, (Reading, MA: Addison-Wesley, 1998), Ch. 4, "Identify Risk".

[26] Dorfee AJ, et al, 1996.

[27] Elaine Hall, *Managing Risk, p.* 101.

[28] Project Management Institute, *A Guide to the Project Management Body of Knowledge 2000 Edition*, (Newtown Square, PA: Project Management Institute, Inc. 2000), Chapter 11.

[29] Elaine Hall, *Managing Risk*.

[30] See the *MSF 3.0 Project Management Discipline*, available at: http://www.microsoft.com/msf