



## **Risk Assessment and Management Process (RAMP)**

State of North Carolina  
Department of Commerce

Information Resource Management  
July 1, 1998

# Risk Assessment Management Process

## Table of Contents

---

<b>RISK ASSESSMENT AND MANAGEMENT PROCESS (RAMP)</b> .....	<b>1</b>
TABLE OF CONTENTS.....	2
PREFACE.....	3
RISK MANAGEMENT PROCESS.....	4
<i>Process Goals and Objectives</i> .....	4
<i>Risk Management Process Methodology</i> .....	4
<i>Risk Categories</i> .....	5
<i>Risk Management Responsibilities</i> .....	6
PROJECT SELF-ASSESSMENT.....	7
<i>License Information</i> .....	7
<i>Purpose</i> .....	7
<i>Project Success Metrics</i> .....	8
<i>Action Planning Guide</i> .....	8
<i>Project Self-Assessment Guidelines</i> .....	9
PROJECT RISK IMPACT ANALYSIS.....	15
<i>Overview of Risk Reporting</i> .....	15
<i>Management Contribution to Risk Management</i> .....	16
<i>Risk Management Response</i> .....	16
<i>Mitigation of Global Risks</i> .....	17
<i>Mitigation of Scope Related Risks</i> .....	17
<i>Mitigation of Timeline-Related Risks</i> .....	17
<i>Mitigation of Cost-Related Risks</i> .....	17
<i>Mitigation of Quality/Performance Risks</i> .....	17
RISK MANAGEMENT PROCESS GUIDELINES.....	18
<i>Identify Risks</i> .....	18
<i>Potential Areas of Risk</i> .....	19
<i>Classify Risks by Type</i> .....	20
<i>Risk Mitigation Plan</i> .....	23
<i>Risk Mitigation Guidelines</i> .....	24
<i>Recording Risk Mitigation</i> .....	24
<i>Risk Profile</i> .....	25
<i>Risk Profile Guidelines Guidelines</i> .....	26
<i>Risk Watch List</i> .....	26
<i>Risk Watch Required Elements</i> .....	27
APPENDIX A – GLOSSARY OF TERMS*.....	29
APPENDIX B – RISK ASSESSMENT QUESTIONS.....	39
APPENDIX C – REFERENCES.....	43

# Risk Assessment Management Process

## **Preface**

Software risk assessment and formal risk management are disciplines that are essential to the application development process. Risk management may be defined as the vehicle used to identify project risk factors using empirical data (or the lack of empirical data) to quantify factors that could cause a project to fail. Webster defines **risk** as “the chance of injury, damage, or loss; hazard.” Therefore, software development project risk may be defined as the “potential realization and cumulative effect of unwanted negative consequences effecting project objectives.”

Risk is not entirely bad. Every major work effort involves risk. However, with risk comes knowledge and opportunity – the opportunity for planning to overcome potential threats to project success. Every project is at risk to fail. The opportunity comes with the project team’s knowledge and understanding of the risk factors and the preparation of a risk management plan to mitigate the risk.

The *Risk Assessment and Management Process* (RAMP) is an automated tool and risk management methodology designed to be used by the IRM staff and the software development project to assist in the definition, analysis, and quantification of project risks which may negatively impact project delivery on-time, within-budget, meeting client business functional requirements, with defect-free software deliverables.

The automated tool provides a baseline project risk assessment using the Kulik and Lazarus Risk Assessment<sup>1</sup> process and then adds a risk analysis module which has been adapted from the State of North Carolina, Office of Information Technology Services (ITS) risk profile system.

Project risk assessment activities must be periodically updated throughout the project system development life cycle. Continuous risk management is essential for several reasons:

1. To monitor and measure progress in risk management,
2. To provide management with visible target dates and milestones in risk management activities,
3. To identify new risk items and issues, and
4. To establish new risk management priorities.

Attached, as Appendix A is a dictionary of data processing terms and definitions that will be used throughout the project system development lifecycle and the risk management process.

---

<sup>1</sup> Kulik and Lazarus is a copyrighted risk analysis tool licensed by the Department of Commerce, Information Technology Services, Information Resource Management.

# Risk Assessment Management Process

## ***Risk Management Process***

### ***Process Goals and Objectives***

The two (2) main objectives of the Risk Assessment and Management Process methodology are to:

1. **Focus attention on minimizing threats in order to achieve the project objectives** by performing a high-level assessment of project risk with all project stakeholders, and
2. **Provide a systematic approach for detail risk analysis and appraisal** by:
  - Identifying and assessing risks.
  - Determining effective risk reduction actions.
  - Monitoring and reporting progress in reducing risk.

The overall goal of this process is to progressively reduce the project's exposure to events that threaten the timely delivery of project objectives by:

- Incorporating approaches into the project plan that minimize, mitigate, or avoid identified and potential risks,
- Developing proactive, contingency plans or risk response plans, and
- Ensuring timely risk responses based on the concise identification of risk occurrence and risk opportunity.

### ***Risk Management Process Methodology***

The risk management process methodology involves five (5) basic steps:

1. ***Identify the risks*** - Understand the typical problems that might adversely affect the project.
2. ***Assess the risks*** - Rank the risks in order of importance based on probability of occurrence, impact of occurrence, and degree of risk certainty.
3. ***Plan the risk response*** – Analyze risk assessment alternatives and modify the project plan to adjust for the risk.
4. ***Monitor the risks*** – Throughout the project, continue to revisit the risk profile, re-evaluate major risks, and update the risk profile with action taken.
5. ***Document lessons learned*** – Learn from the risk identification, assessment, and management process. Use the risk database from past projects to plan current projects, and, use your risk management experience to update the organization risk database.

# Risk Assessment Management Process

## ***Risk Categories***

The following types of risk categories may be used as a high level view of potential risk areas. The major **risk categories** are defined in table 1:

*Table 1 - Risk Categories*

<b><i>CATEGORY</i></b>	<b><i>EXAMPLES</i></b>
Financial	Cost overruns, budget constraints, funding issues
Resource	Availability of people and facilities, attrition, skills limitations
Schedule	Completion date slippage, target date constraints
Technical	Failure to meet performance requirements, new or untested technologies
Management	Inexperienced project manager, project complexity
Communication	Failure to satisfy user requirements / expectations
Operational	Failure to meet usability, trainability, and/or maintainability requirements
Political	Impact of loss of service to citizens, possible exposure and liability to state / county government.
Organizational	Alignment to strategic goals / vision

Refer to Appendix B for a sample list of questions that will probe the major risk categories. ***Caution: The sample list contained at Appendix B may not be comprehensive. The questions are designed to initiate the risk analysis portion of the assessment and may only be indicators of potential risk areas in the system development life cycle. Specific questions may need to be developed and analyzed by the project team based on the project type, scope, and schedule.***

As a key factor in project planning and project outcome, risk management must be included in all project planning activities. At a minimum, the software development project plan should reflect:

- Relationship and contribution of project management to risk management - This section should summarize the key contributions made by various project management components to the reduction of project risks.
- Risk management process - This section summarizes the risk, identification, assessment, analysis, documentation, handling, and reporting process at the overall project and individual function levels.
- Overview of risk management methods and techniques - This is a summary of the methodologies to be used in the project risk management process.

# Risk Assessment Management Process

## ***Risk Management Responsibilities***

Risk management is the responsibility of the Project Manager. However, all project stakeholders should participate in the risk identification and analysis process. Overall the extended project team carries out risk management and mitigation activities.

Refer to Table 2 for a high-level view of basic project risk management responsibilities.

*Table 2 - Risk Management Responsibilities*

<b><i>RISK MANAGEMENT TASKS</i></b>	<b><i>RESPONSIBLE PARTY</i></b>
Overall direction of risk management plan	Project Manager
Plan development and execution of risk management plan	Project Manager
Provide counsel and assistance regarding risk identification/assessment/analysis/handling	Business Analyst, Development Team, Quality Assurance
Risk Watch List	Project Manager
Preparation and issuance of risk reporting	Project Manager as part of normal project status reporting

Members of the application development project team and the Project Manager will conduct risk management activities for technical risks. Monitoring these activities will be the responsibility of the Project Manager, assisted by other members of the project team. These activities include:

- Develop and maintain a project software development plan.
- Develop and maintain a project risk management plan.
- Identify high-level risks applicable to the project through the Kulik and Lazarus ***Project Self-Assessment***.
- Identify additional project-specific risks through the *Risk Analysis* tool.
- Assess and analyze risks.
- Incorporate risk mitigation / avoidance approaches in the Project Plan.
- Maintain, monitor, and update a detailed project risk profile.

# Risk Assessment Management Process

## ***Project Self-Assessment***

### ***License Information***

The Department of Commerce, Office of Information Technology Services (ITS), Information Resource Management (IRM) organization has purchased a license for the “*Project Self-Assessment Kit*” from **Kulik and Lazarus Consulting, Inc.**

### ***Purpose***

The **Kulik and Lazarus “*Project Self-Assessment Kit*”** combines powerful software risk management techniques with innovative statistical models. Results are based on industry research, process standards, and experience managing software projects and conducting risk assessments.

To measure project success metrics, the “*Project Self-Assessment Kit*” uses the individuals involved with the project as the primary source of data. By responding to a common set of specially developed questions, project staff become a source of statistically reliable information. Results of using the “*Project Self-Assessment Kit*” for a project include:

- Measurements for twenty-two Project Success Metrics,
- Identification of project strengths and risk areas,
- Quantified overall project risk level,
- Customized action plans to leverage strengths, and
- Customized action plans to reduce risk.

In project management, **tomorrow’s problems are today’s risks**. With data from the “*Project Self-Assessment Kit*”, a project manager should be able to anticipate and eliminate risks. The goal of risk management is to facilitate project management activities leading to on time, within budget, full-function, and high quality project deliverables. In addition, agency management may use the results of self-assessments to identify targets for process improvement and areas to enhance organizational capabilities.

The analysis tool utilizes input from the major stakeholders of a project effort. Input is obtained from the project sponsor, the I/T project manager, the intended primary client/customer, internal QA staff, and major project stake holders; i.e., ITS operations, telecommunications, and network support. The tool provides an analysis of the twenty-two (22) project success metrics and provides for a comparison to each other and to industry norms.

# Risk Assessment Management Process

## *Project Success Metrics*

The twenty-two (22) areas measured and analyzed by the tool are:

- Requirements Definition
- Requirements Stability
- Technical Complexity
- Schedule Scoping
- Project Plan / Schedules
- Planning Involvement
- Management Sponsorship
- Project Management Tools
- Budget
- Staffing
- Schedule Reality
- Checkpoints
- Risk Management
- Problem / Action Log
- Metrics
- Technical Training
- Change Control
- Development Environment
- Teamwork
- Third-party Involvement
- Process Stability and
- Deployment Planning

In addition to the twenty-two (22) identified metrics, the **Kulik and Lazarus** “*Project Self-Assessment Kit*” for Software Projects also provides and analysis of project:

- Quality Orientation,
- Schedule Orientation,
- Cost Orientation, and
- Overall Risk.

## *Action Planning Guide*

The **Kulik and Lazarus** “*Action Planning Guide*” leads the project through the following steps:

1. Gather Self-Assessment Data,
2. Identify Project Strengths and Risks,
3. Quantify Overall Project Risk, and
4. Develop Action Plans to Leverage Strengths and Reduce Risk

# Risk Assessment Management Process

## *Project Self-Assessment Guidelines*

The roadmap to project self-assessment is shown in Figure 1:

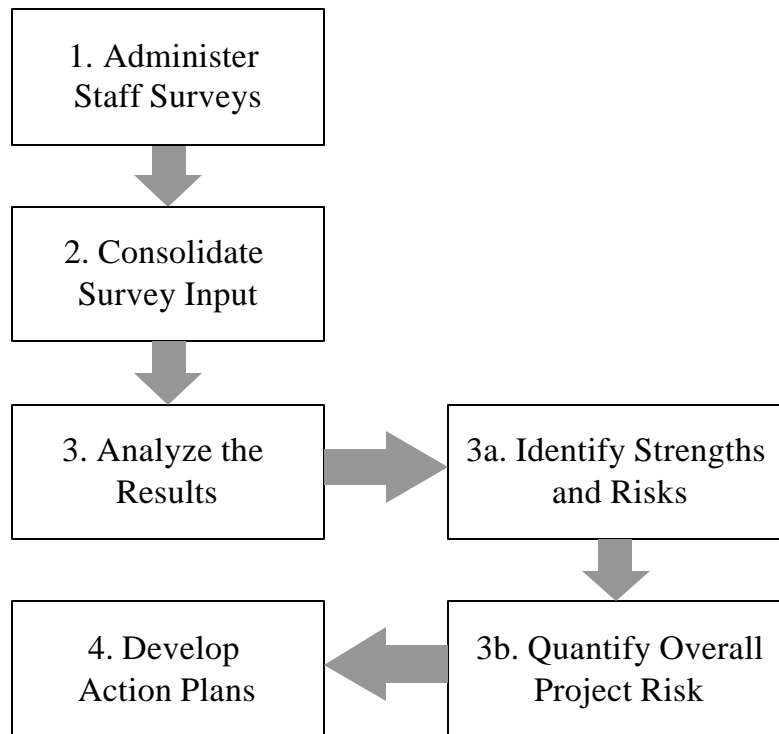


Figure 1

### **Administer Staff Surveys (1)**

Staff surveys will take 10 to 15 minutes for most staff members to complete. The IRM staff recommends that a single 15-minute meeting be scheduled for all staff members to complete the survey. This technique has proven effective to gather consistent, timely feedback. It is easier for project staff – the survey doesn't get added to an already long to-do list. It is also easier for the self-assessment sponsor – project data will be available sooner for analysis.

To administer the Staff Survey, follow these guidelines:

## Risk Assessment Management Process

- Contact the Department of Commerce, IRM Staff at (919) 981-5576 to schedule the “*Project Self-Assessment*”.
- Schedule the *Assessment Survey* meeting.
- Distribute surveys to all those involved in planning and/or implementing the project. This includes (as applicable) engineering and development staff, functional managers, project and / or program managers, quality assurance, integration testing, product planning or product management, cross-functional team members, ITS, etc.

### **Keep survey feedback confidential:**

- *Do:*
  - Tell staff that their feedback is confidential and anonymous.
  - Identify a neutral collection point (e.g., a survey administrator from the IRM staff).
  - Discard any surveys that have been accidentally marked.
- *Don't:*
  - Ask staff to write their name on their survey.
  - Mark surveys with any identifying marks.
  - Comment on feedback from any individual survey.
- Collect all surveys.

### **Consolidate Survey Input (2)**

After all surveys are returned to the IRM Staff, survey answers will be entered into the “Project Self-Assessment Tool”. Surveys will be returned to the project office after data entry is complete.

### **Analyze the Results (3)**

#### *Identifying Project Strengths (3a)*

After data from all staff surveys has been consolidated into the PSAK Software Tool, project strengths and weaknesses may be identified. Strengths will be identified as **Highs** and weaknesses will be identified as **Lows** (refer to figures 2 and 2.1):

# Risk Assessment Management Process

## Highest / Lowest Values

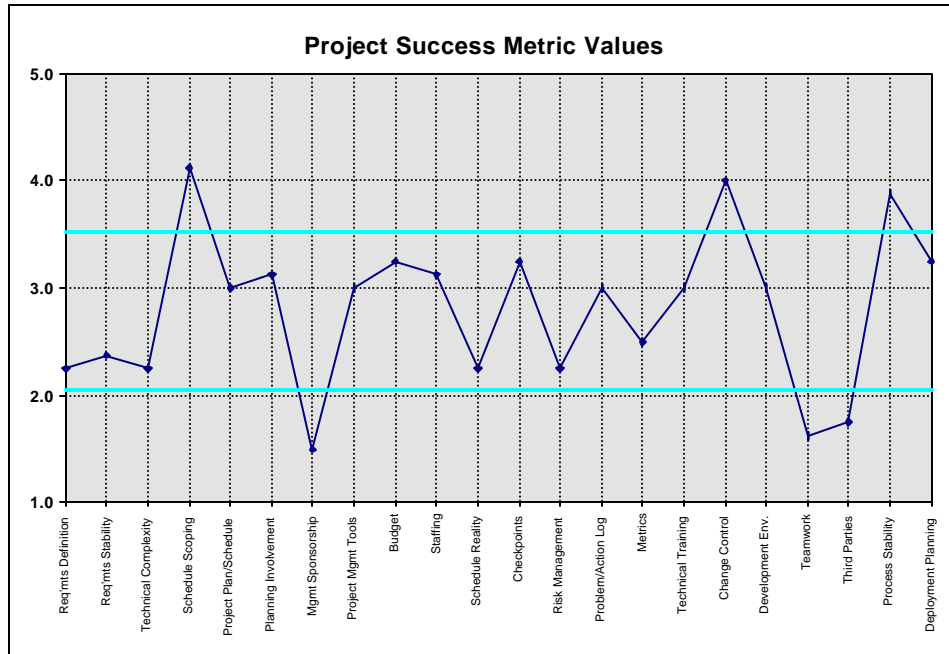


Figure 2

## Most High / Most Low Ratings

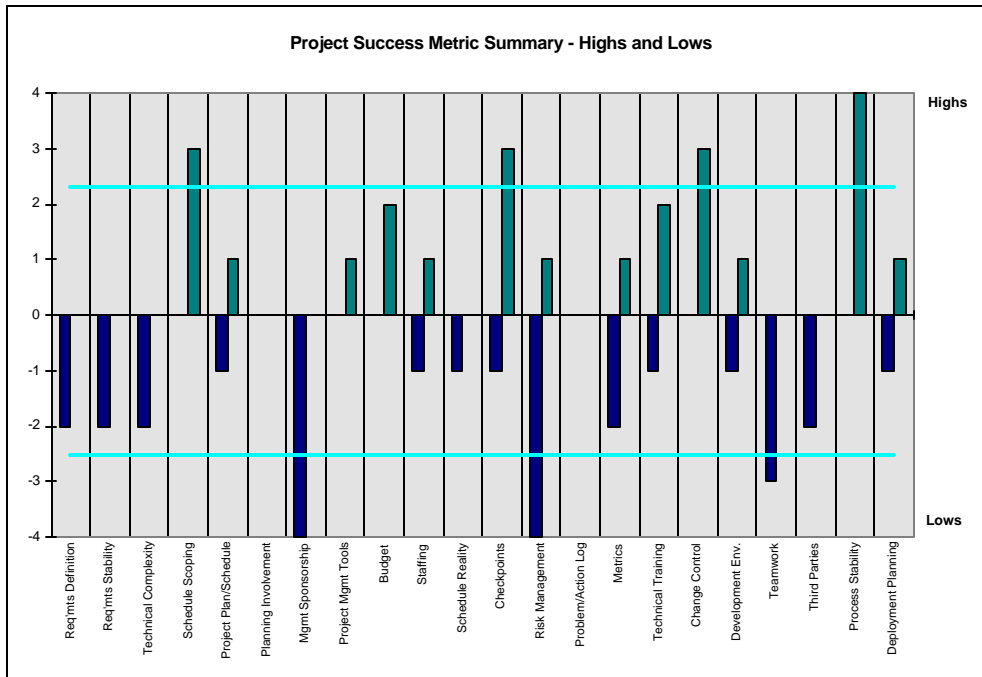


Figure 2.1

# Risk Assessment Management Process

## *Understanding Quality/Schedule/Cost Tradeoffs (3a)*

1. Making tradeoffs between Quality (including content), Schedule and Cost is at the heart of software project management. Frequent tradeoffs are made by project staff, often outside the control of the project manager, which have a significant impact on the project's success.

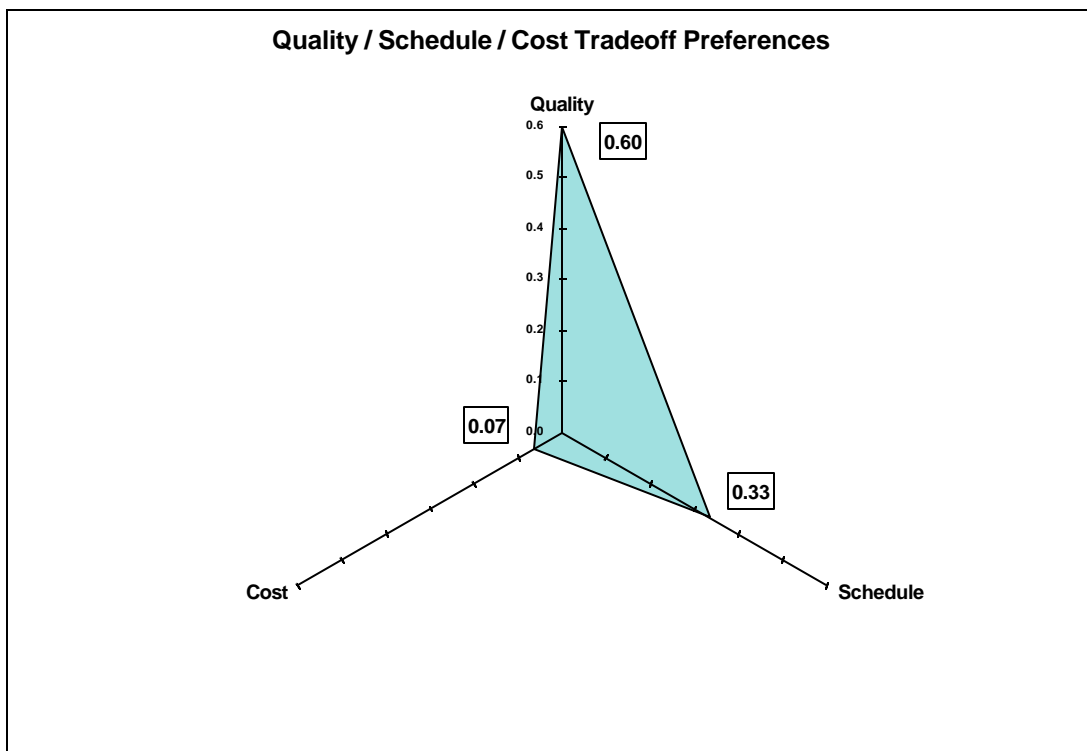


Figure 3

Note, in figure 3, that all tradeoff preferences are measured as an aggregate of individual project staff preferences, rather than individual values. Individual project staff members influence other staff members, providing a system of checks and balances for making project tradeoffs. Figure 3 factors in these checks and balances to describe overall staff preferences.

# Risk Assessment Management Process

## Quantifying Overall Project Risk (3b)

To understand overall project risk, select the worksheet “Overall Risk” in the PSAK Workbook. An example is shown in Figure 4:

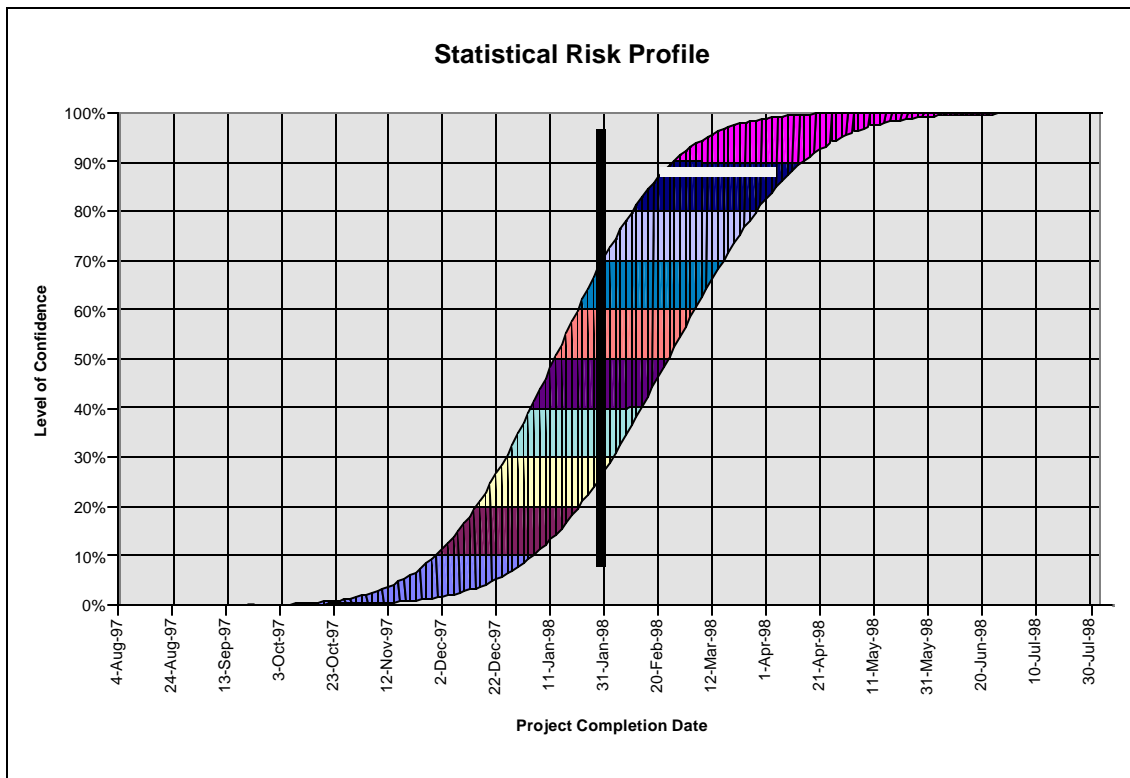


Figure 4

Figure 4 maps the level of confidence in project completion to the scheduled completion date. The upper edge of the curve shows the most-likely relationship, and the lower edge of the curve shows the worst-case relationship.

# Risk Assessment Management Process

## **Develop Action Plans (4)**

After completion of the automated section of the project risk analysis, the IRM staff will generate a project risk analysis report. Copies of the risk analysis report will be provided to all survey respondents and should be used to develop project risk profiles and action plans.

## **Schedule**

Kulik and Lazarus Project Self-Assessments should be conducted as part of the project planning and initiation phase prior to the first independent quality assurance review. Based on the results of the initial assessment, additional risk assessments may be conducted at various milestones in the system development life cycle.

Contact the Department of Commerce, Information Resource Management (ITS/IRM) staff at (919) 981-5576 for more information about the assessment process.

# Risk Assessment Management Process

## ***Project Risk Impact Analysis***

*Project Risk Impact Analysis* is a risk management database that is designed to help the project team identify, prioritize, and communicate project risk. The database is an Excel spreadsheet with detail project risk information (riskreport.xls). Detailed instructions for completing the companion spreadsheet is contained in this section of the document.

Risk impact analysis is a plan for identifying, quantifying, analyzing, mitigating, and reporting project risks. This section includes descriptions of risks and corresponding mitigation actions that have been identified. It guides the project-wide risk reduction efforts. It is applicable to all projects and its requirements affect all functions of a project management office.

The questions "How Much?" and "How Long?" must be answered by most organizations before specific project risk information is known. As a result, project estimates inherently include uncertainties, assumptions, and risks. Successful project planning and implementation requires risk management, change management, and meaningful contingency planning.

Risk management helps to align the expectations of the project stakeholders and the Project Manager regarding project process, issue resolution, and project outcome. Clients often have involuntary risks or constraints imposed upon them. They often are taking project risks they don't even know they are taking due to poor articulation of the risks and their possible impact on the project. As a result, clients are often surprised by negative consequences and unmet expectations. It is the Project Manager's job to identify and to articulate the potential risks and their possible impacts to the client. The clients then assume the risks on a voluntary basis and can be actively involved in assisting with risk management.

## ***Overview of Risk Reporting***

To provide visibility of risks and progress in mitigating them, the following reports should be distributed on a regular basis as part of the normal project status reporting system:

*Table 3 - Risk Reporting Sections*

<b><i>TITLE</i></b>	<b><i>LEVEL</i></b>	<b><i>DESCRIPTION</i></b>
<b><i>Risk Watch List</i></b>	Organization & Project	Lists risks to facilitate monitoring risks and initiating risk responses.
<b><i>Risk Mitigation Plan</i></b>	Organization & Project	Lists avoidance/mitigation actions, if and when risks occur.
<b><i>Risk Profile</i></b>	Project	Displays planned, actual and projected progress in reducing risks.

# Risk Assessment Management Process

## ***Management Contribution to Risk Management***

The keys to effective risk resolution are **early identification**, **communication**, and **risk management**. All issues and risks must be identified and recorded in one place for easy reference by every project team member. Every user and team member must be aware of outstanding issues and accept ownership for their existence (and possible resolution). Finally, the Project Manager must manage and control the issues through an established documented procedure.

The Project Manager must use a structured approach to resolving issues and problems. By clearly defining the underlying problem (root cause), by identifying alternative solutions, and by objectively evaluating the consequences, the Project Manager can minimize adverse effects on the project. Three (3) major issue types are relevant to the any major project:

- ***Business***,
- ***Technical***, and
- ***Team***.

The project stakeholders review the business and technical issues while the team issues remain internal to the project team. When defining and resolving technical issues, priority is a factor. Prioritization of technical issues are handled using a 1-5 scale.

Resolving issues is an ongoing process that occurs throughout the life cycle of any project. Expect, however, that some issues cannot be resolved within the scope of a project. Still, the

Project Manager should identify those issues that cannot be resolved and develop action plans to resolve them at a later time.

When resolving issues, a priority should be assigned to help determine the appropriate resolution. Low, medium, high, and emergency can be assigned to issues associated with the project.

## ***Risk Management Response***

Risk management alternatives include either:

1. **Risk avoidance**,
2. **Transfer / sharing of risk** (insurance),
3. **Prevent the risk**, or
4. **Develop a risk mitigation and / or contingency plan**.

# Risk Assessment Management Process

## ***Mitigation of Global Risks***

The cost / benefit and funding requirements of both potential and encountered risks should be documented in the finalized business requirements.

Appropriate measures should be taken to protect each parties' interests incorporated in contractual arrangements. This will be achieved through the project Statement of Work (SOW) or Document of Understanding (DOU).

## ***Mitigation of Scope Related Risks***

The scope of a project should be completely defined to help avoid inadvertent requirements' omissions, errors, and misunderstandings via Statements of Work and the Project Plan. Management is expected to honor its commitments and to provide the necessary resources required to have a positive and timely outcome. There must be well-defined and enforced acceptance requirements in order to have a successful outcome.

## ***Mitigation of Timeline-Related Risks***

There must be specific support in providing resources outside of the immediate development group via internal / external contract agreements and coordination with organization management. Everyone must agree to multiple phases of a project in order to achieve short-term objectives.

## ***Mitigation of Cost-Related Risks***

The financial situation must continue to be assessed and justified, based on up-to-date business case and economic evaluations. All costs should be reviewed with the section responsible for funding the software development effort.

## ***Mitigation of Quality/Performance Risks***

Acceptance criteria and quality and technical performance criteria (as defined by the requirements and state standards) must be documented. Any State performance standard must be followed under a client/server project.

## ***Risk Management Process Guidelines***

### ***Identify Risks***

Identifying specific risks is occasionally a precarious task. Not all risks can be identified or mitigated contiguously. In this section, you will need to concentrate on identifying underlying problems, based on **visible symptoms**. Symptoms are often the only indication of an underlying project problem or issue. Many symptoms act as a facade to the real problem. The Project Manager must isolate the actual risk and to filter out the symptoms to identify the root cause.

**Note:**

There is no shortcut to identifying problems. Experience, communication, and intuition assist the Project Manager in getting to the "root cause of the risk, problem, or issue."

The general risk management process to be followed begins with reviewing the planning documents that specify the project including:

- Deliverables and work processes,
- Milestones and schedule dates,
- Resource estimates/needs/sources, and
- Performance requirements.

Talk with appropriate stakeholders and other experts to develop a comprehensive list of potential risks. This process may include:

- getting the right people involved,
- staff meetings,
- gathering business requirements,
- analytical sessions,
- scheduling user community meetings, or
- conducting a Kulik and Lazarus high-level project assessment.

Risks or potential risks will also be identified by observation through:

- Management staff interaction, and
- "Reading" personnel actions and reactions.

## Risk Assessment Management Process

### *Potential Areas of Risk*

*Table 4 - Areas of Potential Risk*

<i>NEW TECHNOLOGY</i>	<i>APPLICATION</i>	<i>USER/ CLIENT</i>	<i>PROJECT TEAM</i>	<i>ORGANIZATION</i>	<i>PROJECT MANAGER</i>
Database Software	Project Size	Systems Knowledge	Contract or Full Time	Stability of Organization	Contract or Full Time
Communications Software	Functional Complexity	Change Propensity	Transitional Time	Stability of User Organization	Problem Solving Skills
Programming Language	New vs. Replacement	Turnover of Key People	Technical Skills	Senior Management Commitment	Managerial Identity
Tools or Aids	Quality of Available Information	Client and Customer Relations	Level of Morale	Availability of Champion	Influence Skills
Communications Network	Vulnerability to Change	Readiness for Takeover	Staff Availability	Continued Budget Availability	Achievement Drive
Mainframe	Stability of Business Need	Design Participation	Commitment to Team	Charge-back System	Experience with Users
Testing Resource	Intensity of Business Need	Change process	Applications Knowledge	Project Standards Used	Experience with Application
PCs or Desktops	Organizational Impact	Level of Commitment	Staff Turnover	Accountability for Change	Experience with Organization
Information Center	Interface Exiting Applications	Attitude toward IS	Familiarity with Each Other	Availability of Support Organization	Experience with Technology
Geographic Dispersion	Dependent on other Projects	Applications Knowledge	Staff Conflicts	Extended Team Commitment	Experience with Project Team
Reliability of Personnel	Conversion Difficulty	Acceptance Test Participation	Size of Team	Conflict Resolution Mechanism	Planning Skills
Configuration Management	Implementation Time Frame			Sign-off/approval process	Estimating Skills
Staff / Resource	Personnel Turnover				Communication Skills
					Possibility of Turnover

# Risk Assessment Management Process

## *Classify Risks by Type*

Categorize risks along the lines shown in a risk classification document (table 4), to aid in subsequent determination of risk controllability and selection of appropriate risk mitigation actions.

## *Assess Risks*

**Step 1:** Assess the likelihood of occurrence (**probability of occurrence**) by eliminating any risks which, on reflection, you believe will not occur. Roughly classify the remaining risks as *high*, *medium*, or *low* probability of occurrence.

**Step 2:** Assess the **severity of impact** by:

- evaluating each risk in terms of its possible impact on the project baselines of effort, cost, time (schedule), and requirements (scope, performance, acceptance, quality)
- eliminating any risks which you believe have no or only trivial impact on the baselines
- Roughly classifying the remaining risks as *high*, *medium*, or *low* severity of impact.

**Step 3:** Prioritize the identified risks on the basis of the rough assessments. The contributing factors are the likelihood of occurrence and severity of impact.

**Step 4:** Quantify the risk based on probability by assigning numerical values to various aspects of each risk to provide a consistent basis for combining them into an overall Risk Profile and determining risk mitigation opportunities and actions. Assign a value from “1” to “5” to each risk (based on the likelihood of occurrence) using the scale below:

*Table 5 - Scaling Risk*

<i>ASSESSMENT OF LIKELIHOOD</i>	<i>VALUE SCALE</i>
<i>Very unlikely</i>	1
<i>Somewhat unlikely</i>	2
<i>50/50 chance</i>	3
<i>Highly likely</i>	4
<i>Nearly certain</i>	5

## Risk Assessment Management Process

**Step 5:** Quantify the risk (based on severity of impact) using the table below:

*Table 6 - Assessment of Risk Severity*

<i>ASSESSMENT OF SEVERITY</i>	<i>VALUE</i>
<i>Minor impact on cost, schedule, performance</i>	1
<i>Moderate impact on cost, schedule, performance</i>	2
<i>Significant impact on project baselines</i>	3
<i>Very significant impact on project baselines</i>	4
<i>Disastrous impact, probable project failure</i>	5

**Step 6:** Quantify the risk (in terms of level of controllability) using the table below:

*Table 7 - Risk Controllability Assessment*

<i>ASSESSMENT OF CONTROLLABILITY</i>	<i>VALUE</i>
<i>Essentially avoidable through selected risk mitigation actions</i>	1
<i>Highly controllable through organization or project actions</i>	2
<i>Moderately controllable through organization or project actions</i>	3
<i>Largely uncontrollable by the organization or the project</i>	4
<i>Uncontrollable by the organization or the project</i>	5

**Step 7:** Determine risk mitigation actions. Identify and record potential actions that could be taken in order to avoid or mitigate the individual risks (based on their level of controllability) using the table below:

## Risk Assessment Management Process

*Table 8 - Risk Controllability Rating*

<i>CONTROLLABILITY RATING</i>	<i>TYPE OF MITIGATION</i>
<i>1 or 2</i>	Actions which should be immediately incorporated into the project plan
<i>3 or 4</i>	Actions which should be documented as contingent risk responses to be incorporated in the project plan in the event of the risk occurring
<i>5</i>	None. By definition, such risks cannot be avoided or mitigated

***Caution: The above guidelines are suggestive, not hard and fast. On any given risk, for example, it may be possible to identify actions which should be immediately incorporated into the project to partially reduce the risk, as well as actions which should be treated as contingent risk responses. Risk classification may also change during the system development life cycle.***

For any risks on which multiple, alternative responses were identified, evaluate the responses and select the preferred ones. If time is limited, consider performing only the following:

- Avoidance or mitigation actions to be immediately included in the project plans
- Decomposition of the selected risk responses into their constituent work tasks (the level of detail should be consistent with that used to plan the work in the Project Plan)
- Estimating the resources needed to perform the risk mitigation and scheduling the detailed work activities including:
  - modifying the Project Plan for actions that are to be incorporated immediately
  - determining activity duration (not specific schedule dates) for contingent risk responses

**Note:**

Incorporating these actions may impact the project baselines.

**Step 8:** Prepare a Risk Watch List that summarizes the results of the risks that have been identified. All of the information needed to prepare this document is available (as a result of the preceding work), except that assessment must be made of the target dates for reduction of each risk. Input all of the risk information on the **riskreport.xls** spreadsheet. Making these assessments requires reference to the project schedule to determine when the work associated with the risk is scheduled to be performed.

## Risk Assessment Management Process

**Step 9:** Develop a Baseline Risk Profile. Calculate a Significance Level rating for each risk by summing its ratings for Likelihood of Occurrence and Severity of Impact. Construct an original Baseline Risk Profile by plotting a curve based on the summation of the risk Significance Levels, considering the target dates for reducing each risk by 50% and in total.

**Step 10:** Monitor Risk Status. As work is performed, monitor and assess:

- Progress in reducing risk (e.g., completion of work that achieves the targets of 50% and total risk reduction)
- Occurrence of risks that call for initiation of contingent risk responses
- Effectiveness of implemented risk reduction and risk mitigation actions and any needs to modify these actions.

**Step 11:** Maintain a Risk Watch List. Update the Risk Watch List to reflect the results of monitoring risk status. Also reflect the effect of any project change requests.

**Step 12:** Maintain a Risk Profile. Update the risk profile to reflect the current risk status. This involves the plotting of curves to reflect:

- Actual progress in reducing risks
- Revised risk reduction baseline, considering actual progress, new risks identified, and effects of change orders and re-planning changes.

**Step 13:** Report Risk Status. The Risk Watch List is issued as a regular component of the standard monthly project performance reporting packages (e.g., status reports, project plan milestones, Gantt charts).

### ***Risk Mitigation Plan***

This section defines the actions that need to be taken in order to reduce or eliminate the impact of risks on the project or on individual functions. A Risk Mitigation Plan is done during initial project analysis and planning. Maintain it in connection with the project execution. This process is also utilized in connection with the detailed project planning activities and is updated (as needed) in subsequent cycles of re-planning. It is applicable to all projects and can be applied to ongoing functions of the project management office when relevant.

# Risk Assessment Management Process

## *Risk Mitigation Guidelines*

Risks can arise from any aspect of a project. Thus, a complete identification of all project risks can only be obtained by involving a sufficient number of people to ensure that in-depth competence and experience is applied to the process for all significant aspects of the project scope.

Some project risks can be identified by simply deducing the defined project risks that are applicable to the project. It may be necessary to restate these risks in the context of the project scope. Other project risks can only be identified by carefully analyzing the project plans and requirements.

Some of the risk mitigation actions can be incorporated into the Project Plan in conjunction with detailed project planning activities. Other risk mitigation actions represent contingency plans to be implemented only if the risk actually occurs.

A secondary use of the Risk Mitigation Plan occurs if and when implemented risk responses do not prove effective. When this happens, the Risk Mitigation Plan provides information on other, alternative risk responses that should be reconsidered for implementation.

## *Recording Risk Mitigation*

Table 9 - Risk Mitigation Table is self-explanatory, except as follows:

1. **Category** - Project Management normally specifies the standard categories of risks. The categories that will be used are found in Table 1;
2. **Object** - The object, task, phase, or activity (at the project level) to which the risk applies;
3. **Severity** - A subjectively assigned numerical rating from low to high of the expected level of impact on the project if the risk occurs (see Table 6 - Assessment of Risk Severity);
4. **Alternative responses** - Detailed plans (or cross-references to attached detailed plans) that specify the alternative sets of actions that can be taken to avoid or mitigate the identified risks;
5. **Rank of Response** - The preferred ranking of the alternative responses starting at “1” (most preferred). Refer to Table 8 for detailed descriptions of control rank responses;
6. **Response Taken** - “Contingent” is entered if the response is only to be acted upon, when the risk occurs;

## Risk Assessment Management Process

7. **Assign responsibility** - Assign the risk to the appropriate individual. This does not need to be tracked in the “Suggested Risk Mitigation Table” but may be included in the Comments section and must be included in the project plan with the associated resources.
8. **Comments / Closure** - All risks need to come to a conclusion, even if that conclusion is “no action taken”. Risks requiring a “developed” solution will be reflected in the project plan.

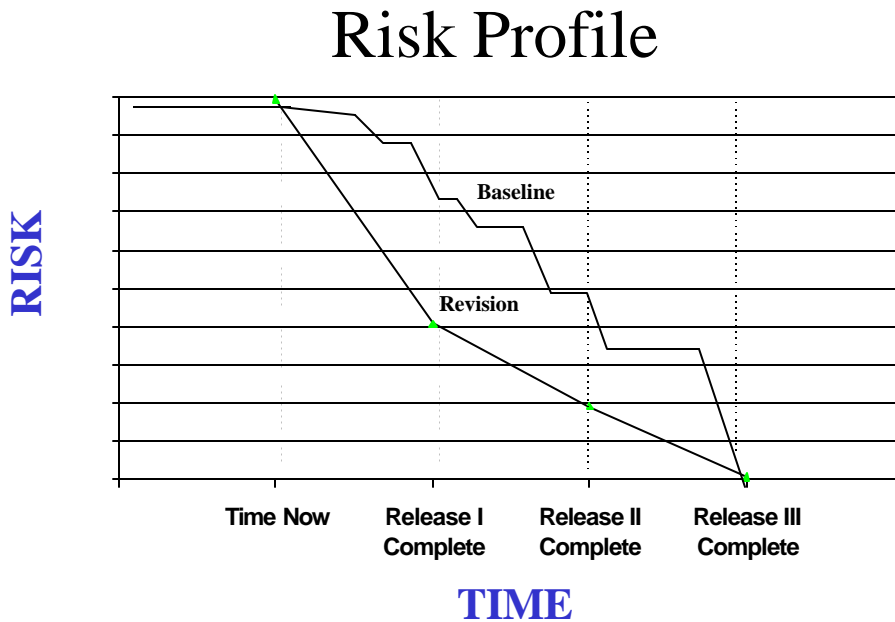
A suggested Risk Mitigation Table format is defined in Table 9.

*Table 9 - Risk Mitigation Table Format*

<i>Category</i>	<i>Object</i>	<i>Severity</i>	<i>Impact Area</i>	<i>Alternative responses</i>	<i>Rank of Response</i>	<i>Response Taken</i>	<i>Comments Closure</i>
<b>Schedule</b>	Case Screen not Delivered on time	4	Call Reception	Wait until Complete	2	Build Bridge to existing system	Waiting Management Approval

### *Risk Profile*

The Risk Profile graphically portrays the project’s exposure to risk. It shows the planned, projected (if different from plan), and actual risk reduction achieved as the project progresses. The Risk Profile is created from the Risk Watch List.



*Figure 5 - Graphical Risk Profile*

# Risk Assessment Management Process

## ***Risk Profile Guidelines***

The Risk Profile risk reduction curves are determined as follows:

**Step 1:** An overall numerical measure is established for each risk. Typically, this is computed by multiplying the Estimated Level of Impact Rating times Level of Confidence Rating where:

- The Level of Impact Rating is a number that represents the severity of the impact if the risk occurs.
- The Level of Confidence Rating is a number that represents the expected probability that the risk will occur.

**Step 2:** Dates are established representing the times when each risk is planned to be reduced (first by 50% and then in total).

**Step 3:** The values for these measures are reduced as progress is made in reducing the risks.

**Step 4:** The results of the above calculations are summed for the project by time period (usually months), taking into consideration:

- planned Risk Reduction, to derive the planned risk profile
- achieved Risk Reduction, to derive the actual risk profile
- Projected Risk Reduction, to extrapolate a projected risk profile (if actual varies significantly from plan).

One option is to show two planned risk reduction curves, the original plan, and the current or revised plan. Attached, as Appendix C is a detailed list of references for additional risk management research.

## ***Risk Watch List***

A *risk watch list* is a list of current risks that typically shows type of risk, level of impact, importance, ways of identifying and handling the risk, time frame for risk reduction, responsibility for management of the risk.

# Risk Assessment Management Process

## *Risk Watch Guidelines*

One option is to include a rating for each risk that is a combination of the **Level of Impact** and **Level of Confidence** ratings.

Another option is to identify and include in this Section “Risk Triggers”, which are symptoms to watch for that signal potential or actual occurrence of the risk.

A simple scheme should be used to quantify risks. The quantification process is somewhat subjective, regardless of the method used to assign the numerical values. Using a more complex quantification scheme will probably not do much to reduce this inherent subjectivity.

Consideration should be given to devising a scheme for quantifying the impact of joint occurrence of multiple, closely related risks. The effect of such occurrences may be much more significant than is implied by simply summing their individual values. The likelihood of such occurrences is usually calculated by multiplying the individual risks’ estimated probability of occurrence by each other. The usual handling of joint risks is:

- to combine them and reassess the resulting, more global risk
- To define an additional risk described as a joint occurrence risk and assess it in terms of the incremental impact of the joint occurrence over and above that of the individual risks.

Consideration should also be given to relating each risk to the corresponding level of Project plan. This will prove helpful in keeping management attention to each risk at an appropriate level of detail.

## *Risk Watch Required Elements*

The typical data shown in Table 10 - Suggested Risk Watch List, is self-explanatory, except as follows:

1. **Risk Category** - Type of risk, based on standard categories established by Project Management. One typical categorization scheme is:
  - **Financial** - Almost everything results in cost. Limit these entries to estimating errors, budget effecting overruns.
  - **Resource** – Most application development efforts involve the use and availability of people and skills.
  - **Schedule** - Anything that directly effects the schedule as defined in the Project Plan (e.g. estimating/scheduling errors, resource availability problems, and overruns).
  - **Technical** - Anything that is directly related to the technology chosen to provide a solution (e.g. requirements complexity and/or changes, immature technology, integration problems).

## Risk Assessment Management Process

- **Management** – Project management skills or organizational management focus and commitment are essential elements of all software development efforts.
  - **Communication** – The inability to understand user requirements and avoid project surprises are key project success measures.
  - **Operational** - Implementation problems due to conflicts, poor training, physical resource unavailability.
  - **Political** – Effect on the citizens and citizen services.
  - **Organizational** - Events outside the project such as marketplace developments, regulatory changes and strategy changes.
2. **Related Work** - When applicable, a cross-reference to the work that gives rise to the risk. In a project-level document, it will normally be a deliverable associated with the risk.
  3. **Risk Response** - A summary statement of the risk response(s) which is preferred or which has been initiated. Note that the details of the response are spelled out in the Risk Mitigation Plan.
  4. **Level of Impact, Level of Confidence, Level of Control** - Judgmentally assigned numerical ratings of the expected severity of the effect, estimated probability of occurrence, and expected ability to control each of the identified risks. Any number scale can be used, but a 3-point scale (i.e. "1" to "3") is usually sufficient and does not imply an undue level of precision.
  5. **Date to Reduce by 50% and Completion Date** - These dates show the risk reduction targets for management control purposes. They also provide the data needed to plot the time axis of the Risk Profile.

### *Risk Watch List Suggested Format*

*Table 10 - Suggested Risk Watch List Format*

CATEGORY	DESCRIPTION	RESPONSE	TYPE	SEVERITY	LIKELIHOOD	SIGNIFICANCE (SEVERITY + LIKELIHOOD)	LEVEL OF CONTROL	DUE DATE
Schedule	Case screen not delivered on time.	Build bridge to existing system	I	4	5	9	5	Change Request pending
Technical	Cannot support MobileCom <sup>TM</sup> alpha paging; interactive software does not run under UNIX	Build an Internet interface to accomplish alpha paging	I	3	5	8	1	Change Request pending

# Risk Assessment Management Process

## **Appendix A – Glossary of Terms\***

### **A**

**Acceptance Criteria** – The list of requirements that must be satisfied prior to the customer accepting delivery of the product.

**Acceptance Test** – Formal user performed testing performed prior to accepting the system (sometimes called client acceptance test or user acceptance test).

**Acquisition** – Generic term for hardware, software, or services acquired from an outside vendor or contractor.

**Action Plan** - A plan that describes what needs to be done and when it needs to be completed. Project plans are action plans.

**Activity** - A specific project task, or group of tasks, that require resources and time to complete.

**Adaptive System** – Describes software that has flexibility as the primary design point.

**Application** – Generic term for a program, or system, that handles a specific business function.

**Application Software** – A complete, self-contained program that can perform work for a user. This is in contrast to system software such as an operating system, server processes, and libraries that exist in support of application software.

**Approval Cycle** – Process of gaining funding and management approval prior to project initiation.

**Architecture** – Imposes order and makes interconnections possible. Generally defined as an intermediate step between initial requirements and business functional specifications during which the entire complex of hardware, software, and design considerations are viewed as a whole. Refers to a blueprint for evolving a technical infrastructure.

**Assessment** – A general term for the formal management review of a process.

**Audit** - A formal and detailed examination of the progress, costs, operations, results, or some other aspect of a project or system performed by an independent party.

**Availability** – The portion of time that a system that is scheduled to operate actually can be used as expected.

### **B**

**Baseline Plan** - The initial approved plan to which deviations will be compared as the project proceeds.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

**Batch** – A term describing a method of operating computers. This method takes groups of transactions, executes them, and returns the results, all without human intervention.

**Backbone** – A high-speed computer network designed to interconnect lower-speed networks or clusters of dispersed user devices.

**Baseline** – A specification, or product, that has been formally agreed upon which serves as the starting point against which progress will be judged.

**Bench Mark** – A standard figure of merit which measurements or comparisons may be made.

**Bridge** – Devices that connect two separate networks. Once bridging is accomplished, the bridge makes interconnected networks look like a single network.

**Budget** – A planned sequence of expenditures over time with costs assigned to specific tasks and activities.

## C

**CASE – Computer Aided Software Engineering** - Systems that attempt to automate some or all of the tasks involved in managing, designing, developing, and maintaining software systems.

**Change Management** – The formal process of recording, analyzing, estimating, tracking and reporting of changes to the project baseline business functional requirements.

**Checkpoint** – A point in the development process at which project state, status, and results are checked, recorded, and measured.

**Client/Server System** – Primarily a relationship between processes running on separate machines. A client initiates the dialog by sending requests to the server asking for information or action.

**Confidence Level** - A level of confidence, stated as a percentage, for a budget or schedule estimate. The higher the confidence level, the lower the risk.

**Configuration Management** – Methodical storage and recording of all software components and deliverables during development.

**Connectivity** – Refers to the ability to send and receive information between locations, devices, and business services.

**Contingency Plan** - An alternative for action if the project does not proceed according to plan or if the expected results are not achieved.

**Control** - A process for assuring that reality, or actual performance, meets expectations or plans.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

**Cooperative Processing** – Computing that requires two or more distinct processors to complete a single transaction.

**Cost / Benefit Analysis** – A formal study in which the development, execution, and maintenance costs for a project are matched against the anticipated value of the product.

**Critical Activity** - A task, activity, or event that, if delayed, will delay another important event - probably the completion of the project or a major milestone in the project.

**Critical Path** – Derived from the PERT method, this term implies the set of activities that must be completed in sequence and on time if the entire project is to be completed on time. A missed task on the critical path will cause a product delivery delay. This is the longest time for the project from beginning to end.

**Critical Path Method (CPM)** - One of the two most common forms of networking systems. CPM uses a one-time estimate for creating a project schedule.

## D

**Data** – Describes the numbers, text, graphics, images, and voice stored in a form that can be used by a computer.

**Data Warehouse** – Where you consolidate and store data from many sources.

**Deliverable** – A tangible, physical object that is the output of a software development task.

**Dependency Diagram** - Another name for a network or precedence diagram that shows the dependencies among tasks.

**Design** – The tasks associated with specifying and sketching the features and functions of a new application prior to coding.

**Development Project** – The sum of all tasks and activities necessary to build a software product.

**Document of Understanding** – A formal agreement between two parties. A contract which is sometimes referred to as a Statement of Work (SOW).

**Documentation** – The printed and displayed materials which explain an application to a user.

**Duration** - The period of time over which a task takes place. Duration establishes the schedule for a project.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

### E

**Effectiveness** - A measure of the quality of attainment in meeting objectives.

**Efficiency** - A measure of the volume of output received for the input used.

**Effort** - The amount of work or labor (in hours or workdays) required to complete a task.

**Environment** – The set of tools and physical surroundings in which software is developed.

**Estimate** – A predicted total of expenditures required to complete a task, activity, or project.

**Exit Criteria** – The set of conditions that must be met prior to completing a project phase or application.

### F

**Feasibility Project** – A project designed to prove, or disprove, the appropriateness of the technology solution under existing constraints (sometimes called “proof-of-concept” project).

**Float** - The amount of time for a task to be freely scheduled without affecting other tasks in the project.

### G

**Gantt Chart** – A method of displaying overlapped and partially concurrent activities by using horizontal lines to reflect the time required by each activity. The chart, named for Henry Lawrence Gantt, consists of a table of project task information and a bar chart that graphically displays the project schedule to be used in planning and tracking.

**Gateway** – Hardware or software that translates between two dissimilar protocols.

**Granular** – Describes the art of writing small modules of code and / or objects.

**Graphical User Interface (GUI)** – A manner of presentation that makes use of windows, icons, menus, pointers, and scroll bars.

### H

**Hardcode** – An informal term that describes a programming technique where data or procedures are specifically written into the program instructions.

**Hardware** – Physical equipment used to process, store, or transmit computer program data.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

### I

**Independent Review** – A formal examination of a project conducted by an organization other than the development organization.

**Information** – The meaningful interpretation of data.

**IRMC** – Information Resource Management Commission.

**Integration** – Describes the work, or device, required to connect two different systems that were not originally designed to work together.

**Integration Test** – Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them.

**Interface** – A connection between two devices or systems.

**Interoperability** – The ability to have applications and computers from different vendors work together on a network.

**Intranet** – An Internet network behind a firewall.

**Issue** – A problem to be solved or a decision that has not been made.

### J K L

**Lag** - The amount of time after one task is started or finished before the next task may be started or finished.

**Lead** - The amount of time that precedes the start of work on another task.

**Local Area Network (LAN)** – A communications system confined to a limited area, typically a building, occasionally a group, and linking computers together via cable.

### M

**Maintenance** – Refers to the ongoing activity that keeps software functioning in a technical and business environment (production).

**Methodology** – A set of formal protocols followed when performing a task.

**Middleware** – Software that hides the complexity of the networked computing environment from the users and application programmers.

**Milestone** – A major checkpoint in the activities involved in a project. A clearly defined point in a project that summarized the completion of a related set of tasks.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

**Model** - A way of looking at reality, usually for the purpose of abstracting and simplifying it to make it understandable in a particular context.

**Modular Programming** – Programming that has as its fundamental assumption that a large piece of software should be separated into its constituent parts or modules thereby making for easier and faster development and maintainability. Modules were traditionally called subroutines or functions and now are often called objects.

## N

**Network** – Describes the physical hardware and software connections between computers allowing information to be shared and electronic communications to take place.

**Network Diagram** - The logical representation of tasks that defines the sequence of work in a project.

**N-tier Architecture** – Describes a method for dividing an application into a series of distinct layers to provide for ease of maintenance and flexibility.

## O

**Operating System** – System software that controls data storage, input and output to and from the keyboard, and the execution of applications written for it. It performs base services: prioritizing work, scheduling, memory management, etc.

## P

**Padding** - A standard project management tactic used to add extra time or money to estimates to cover for the uncertainty and risk of predicting future project activities.

**Package Acquisition** – The purchase, or lease, of software from an outside source.

**Path** - A sequence of lines and nodes in a project network.

**PERT – Project Evaluation and Review Technique** - The PERT method uses the concepts of milestones, activities, and slack time to calculate the critical path. The chart, which resembles a flow chart, depicts a box to represent each project task and a line connecting two boxes to represent the relationship between tasks.

**Phases** – The divisions of a software development life cycle into discrete stages (e.g., requirements, design, code, test, etc.).

**Planning Project** – A project intended to gather, or predict, the sequence of activities and resources needed to complete a work effort.

**Platform** – The hardware and support software with which a program is intended to operate.

## Risk Assessment Management Process

### Glossary of Terms\* (continued)

**Precedence** - When one task must be completed before another task can be started, the first task is said to have precedence over the other.

**Process** – The step by step sequence of activities (systematic approach) that must be carried out to complete a project.

**Programming** – The art of writing, in a computer understandable language, a set of instructions that produces software.

**Project** – The combined resources (people, machines, materials), processes, and activities that are dedicated to building and delivering a product to a customer.

**Project Duration** - The time it takes to complete the entire project.

**Project Management** - The combination of systems, techniques, and people required to successfully complete a project on time and within budget.

**Project Manager** – The senior person responsible for the entire project.

**Project Plan** – A formal document that describes the technical and management approach to be followed for a project.

**Project Sponsor** – The department “customer” who will authorize project initiation, and who will receive, accept, and use the software product or service.

**Protocol** – A set of rules and specifications that describes how a piece of software will behave and how other pieces of software must behave in order to work with the first piece of software.

### Q

**Quality** (Product) - Conformance to business functional requirements with defect-free products. Quality reflects both the completeness of software or system features and functions, and error-free operation.

**Quality** (Process) – Verification and validation to established policies, standards, procedures and guidelines for software development.

**Quality Assurance** – Within the State of North Carolina, the process tracking and oversight function for monitoring project performance, adherence to commitments, and budget requirements. Performed under the control of the Department of Commerce, Information Resource Management staff.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

### R

**Regression Test** – Selective re-testing to detect errors or faults introduced during modification of a system.

**Relational Database** – A collection of data that is organized into tables so that relationships between and among data can be established.

**Resource Leveling** - The process of shifting resources to even out the workload of team members.

**RFP - Request for Proposal** - Formal statement by a department that they are soliciting enterprises to bid on a contract for a program, system or service.

**Requirements** – The statement of needs by a user that triggers the development of a program, system, or project. May be called business functional requirements or requirement specifications.

**Research and Development Project** – A definition of a project type essentially exploring options for developing new systems or work products.

**Risk** – The probability that a project will experience undesirable events, which may create, cost overruns, schedule delays, or project cancellation. The identification, mitigation, tracking, and management of those elements creating the risk situation.

**Risk Analysis** - An evaluation of the feasibility or probability that the outcome of a project will be the desired outcome.

### S

**Scalable** – A term describing an architecture or software that can handle expansion in the use as the need arises without adversely impacting systems management and operations.

**Scope** - The magnitude of the effort required to complete a project.

**Server** – A computer on a network that makes applications, print services, data, and communications available.

**Slack** - see float.

**Software** – Computer programs, systems, and the associated documentation that describes them.

# Risk Assessment Management Process

## Glossary of Terms\* (continued)

**SDLC - Software Development Life Cycle** – The period of time that begins with the decision to develop a software product and ends when the software is delivered.

**Software Development Process** – The process by which user needs are translated into a software product.

**Specifications** – General term for the wide variety of paper-based descriptions of a program or system.

**Stakeholders** - People who have a personal or agency interest in the end results of a project.

**Standalone** – Describes a computer workstation where the computer is not connected to any other computer on a network.

**Statement of Work (SOW)** - An integrated set of task descriptions, goal descriptions, risks, and assumptions that accompany the evolving master project plan during development.

**Strategic Plan** – The long range plan where the horizon is usually three to five years time span.

**Subcontract** - Delegating tasks or sub-projects to contractors or other organizations.

**System** – A linked collection of programs, or components, that perform a generic business or technical function.

**System Test** – The final stage of testing on a completed project (prior to client acceptance test) when all hardware and software components are put together and tested as a whole.

**SDLC - System Development Life Cycle** - The complex of tasks and deliverables that are organized toward developing software systems.

## T

**Tactical Plan** – Specific improvements, or changes, that will be carried out in a fairly short time span (usually twelve (12) months).

**Task** - A cohesive unit of work on a project (usually 40 to 80 hours of effort).

**Task Description** - A description that defines all the work required to complete a project task or activity including input, output, expected results, and quality specifications.

**Test Plan** – A document that describes the scope, approach, resources, and schedule of intended test activities.

# Risk Assessment Management Process

Glossary of Terms\* (continued)

**Testing** – The set of defect removal tasks that include execution of all, or part, of an application on a computer.

**Topology** – The map or plan of a network.

## U

**Unit Test** - The testing carried out personally by individual programmers on their own code.

## V

## W

**Wide Area Network (WAN)** – A network where the computers are separated by significant distances and telecommunications links are implemented.

**Work Breakdown Structure (WBS)** – A formal analysis of the activities, tasks, and sub-tasks that must be accomplished to build a software project. A product or activity oriented hierarchy tree depicting the elements of work that need to be accomplished in order to deliver a product.

**Workstation** – Any machine with all of its installed storage, processing, and communications that can be either standalone or networked.

## X

## Y

## Z

\* Definitions were extracted from **Assessment and Control of Software Risks** by Capers Jones (1994); **Managing Software Development Projects (Second edition)** by Neal Whitten (1995); **IEEE Standards Collection: Software Engineering** (1997 Edition); **Best Practices in IT Architecture Planning and Implementation** by Larry DeBoever; **Essential Client/Server Survival Guide** by Robert Orfali; and **The Complete Idiot's Guide to Project Management** by Sunny and Kim Baker.

# Risk Assessment Management Process

## **Appendix B – Risk Assessment Questions**

The following questions are designed to assist you in the identification of project risk items. The questions are designed to generate a risk analysis process within the project team. These questions are not the only project risk items. However, the questions do represent a comprehensive assessment of potential project risks. Use the questions in a brainstorming session to elicit comments from team members. Remember, throughout the project life cycle, the risk profile may change. Periodically, review the questions and verify and validate your responses. Update your risk profile to reflect changes.

### **Category: Financial Risk**

1. Is project funding based on work-level estimates?
2. Is project funding secured?
3. Is project funding sufficient?
4. Has a cost / benefit analysis been performed?
5. Has senior management approved the cost / benefit analysis?
6. Are expected benefits verifiable?
7. Is there a detailed budget for the project?
8. Is there a contingency plan for budget overruns?
9. Has the value of the project been discussed with the client and the users?
10. What could make the project go over-budget?
11. What are the risks to the agency if the project fails?
12. What business-related problems would make this project fail?
13. Is the project estimate realistic?
14. Is the project estimate achievable?

### **Category: Resource Risk**

1. Are key personnel needs identified in the project plan?
2. Is there a contingency plan for resource variances?
3. Are all project team members trained?
4. Are project team skill requirements clearly defined?
5. Are project team assignments based on resource skill requirements?
6. Does the project team possess the skills necessary to complete the project?
7. Does the project team understand their roles and responsibilities?
8. Is their sufficient manpower to complete the project?
9. Has adequate technical and professional training been made available to the project team?
10. Does the project team possess the skills to complete the project?
11. Are the project engineers, technical staff, and infrastructure support staff qualified?
12. Are vendors well established with a strong financial background and good track record?
13. Will key project staff leave before the project is complete?
14. Is the development team at a central location?

# Risk Assessment Management Process

## Appendix B – Risk Assessment Questions (continued)

### **Category: Schedule Risk**

1. Is there a detailed project plan at the task level?
2. Have estimates been provided at the task level?
3. Has the project critical path been identified?
4. Is there a contingency plan for schedule variances?
5. Is actual progress regularly compared to the project schedule?
6. What would keep the project from completing on time?
7. Is the project schedule realistic?
8. Is the project schedule achievable?

### **Category: Technical Risk**

1. Are the business functional requirements stable?
2. Are the business functional requirements defined?
3. Have project limitations been discussed with the client?
4. Will the appropriate technology be used to support project efforts?
5. Has the application architecture been developed and documented?
6. Will the project follow a formal methodology?
7. Has the methodology been tested and certified?
8. Does the project team understand the methodology?
9. Are all business and technical requirements verified and validated?
10. Does the project team provide input to proposed changes in the plan?
11. Are team walkthroughs and formal inspections conducted for key project deliverables?
12. Are all project problems identified, documented, and acted upon?
13. Is the technology new or extremely complex?
14. Are the project team members knowledgeable on the proposed technology environment?
15. Do the key technologies provide an appropriate technology for system design?
16. Are all interfaces identified?
17. Has a project work plan been developed for the entire system development lifecycle?
18. Have critical project milestones and checkpoints been defined?
19. Has the appropriate system development lifecycle been selected?
20. Has a change management process been defined?
21. Will business functional requirement (scope) changes affect the project outcome?
22. Is the organization ready to support the new application?
23. Do process policies, standards, procedures, and guidelines exist?

# Risk Assessment Management Process

## Appendix B – Risk Assessment Questions (continued)

### **Category: Project Management Risk**

1. Does upper management support the project effort?
2. Does upper management share responsibility for ensuring project success?
3. Has senior management approved the project?
4. Have all project stakeholders been identified?
5. Has upper management provided the support infrastructure necessary to ensure successful project deliver?
6. Will upper management support the project manager's decisions?
7. Is the project manager experienced?
8. Does the project manager have deep relevant experience?
9. Is there a detailed plan (including time, schedules, milestones, and resource requirements) for completion of the project?
10. Will the projects be managed at the task level?
11. Are project tasks defined at increments of 40 – 80 hours of effort?
12. Do the people implementing the project understand project objectives?
13. Are all important aspects of the project monitored?
14. Are all important aspects of the project measured (planned versus actual)?
15. Are all checkpoints and milestones defined?
16. Does the project have a quality management plan?
17. Will business processes need to be re-engineered?
18. Have formal client acceptance criteria been defined?

### **Category: Communication Risk**

1. Are the project goals in line with the organization goals?
2. Are the project's goals and objectives verifiable, defined, and clearly stated?
3. Are project outcomes clearly defined?
4. Have the basic goals of the project been communicated to the team?
5. Does the project team agree with the goals?
6. Are all external (outside the Agency) project stakeholders identified?
7. Do all project stakeholders accept their project responsibilities?
8. Has the client had an opportunity to provide input early in the system development life cycle?
9. Are all project stakeholders kept informed of project status?
10. Has adequate project presentation been made to the client and user communities?
11. Do the users know whom to contact in the event of problems?
12. Are there regular meetings with project stakeholders to monitor project progress?
13. Does the project team receive feedback from status meetings?
14. Are the results of informal and formal project reviews shared with project stakeholders?
15. Are brainstorming sessions held with the project team to determine where problems are likely to occur?
16. Are all "open issues" reported and tracked?
17. Have major project risk factors been identified?

# Risk Assessment Management Process

## Appendix B – Risk Assessment Questions (continued)

### **Category: Operational Risk**

1. Is there adequate project documentation to permit use by the client?
2. Have potential users been contacted about the usefulness of the project?
3. Are all project problems logged, prioritized, estimated, and acted upon in a systematic manner?
4. How confident are you that you are producing a system to meet the end user's needs?
5. Is the user's business environment stable?
6. Have all technology options been thoroughly investigated and analyzed?
7. Will the project comply with the State Technical Architecture?
8. Will the existing computing environment support the application?
9. Will new hardware need to be procured?
10. Have networking considerations been addressed?
11. Is the application architecture an extension of the installed base?
12. Is the application architecture compatible to the installed base?
13. Is the proposed hardware / software environment in production today?
14. Are backup / restart procedures clearly defined and tested?
15. Are all project baseline deliverables under configuration management?
16. Are all business functional requirements testable?

### **Category: Political Risk**

1. Is the project defined from legislative mandate?
2. What is the impact of non-delivery of project objectives for the citizens of the State?
3. What is the liability to the State for non-delivery of function?
4. What is the potential exposure to news / media coverage for failure to deliver?

### **Category: Organizational Risk**

1. Does the project align with the Agency's overall business strategy?
2. Are the expected outcomes clearly defined?
3. Have all project stakeholders been defined?
4. Have metrics been established to verify completion of each phase?
5. Is senior management committed to the project objectives?
6. Has the impact of late delivery been analyzed?
7. Has the impact of cost overruns been analyzed?
8. Has the impact of delayed functional delivery been analyzed?
9. Does the project comply with the State Technical Architecture?

## **Appendix C – References**

**The Healthy Software Project: A Guide to Successful Development and Management**, Mark Norris, Peter Rigby, and Malcolm Payne. John Wiley and Sons, 1993.

**Software Quality: Analysis and Guidelines for Success**, Capers Jones. International Thomson Computer Press, 1997.

**Software Systems: Failures and Success**, Capers Jones. International Thomson Computer Press, 1996.

**Death March: The Complete Software Developer’s Guide to Surviving “Mission Impossible” Projects**, Edward Yourdan. Prentice-Hall PTR, 1997.

**Managing the Software Process**, Watts Humphrey. Addison-Wesley, 1993.

**The Capability Maturity Model: Guidelines for Improving the Software Process**, Watts Humphrey, etal. Addison-Wesley, 1995.

**Measuring the Software Process: A Practical Guide to Functional Measurements**, David Gamus and David Herron. Yourdan Press Computing Series, 1996.

**Software RX: Secrets of Engineering Quality Software**, Rodney C. Wilson. Prentice-Hall PTR, 1997.

**Managing Software Development Projects: Formula for Success**, Neal Whitten. John Wiley and Sons, Inc., 1990.

**Managing Software Development Projects: Formula for Success (Second Edition)**, Neal Whitten. John Wiley and Sons, Inc., 1995.

**Quality Assurance for Information Systems: Methods, Tools, and Techniques**, William E. Perry. John Wiley & Sons, Inc., 1991.

**Software Runaways: Lessons Learned from Massive Software Project Failures**, Robert L. Glass. Prentice Hall PTR, 1998.

**Project Management: A Managerial Approach**, Jack R. Meredith and Samuel J. Mantel, Jr. John Wiley and Sons, Inc., 1995.

**Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities**, R. Max Wideman. Project Management Institute, 1992.

Appendix C – References (continued)

## Risk Assessment Management Process

**The Complete Idiot's Guide to Project Management**, Sunny and Kim Baker. Alpha Books, 1998.

“Enterprise Computing: Avoiding the Pitfalls of Risk”, Margaret Steen. **InfoWorld**, December 29, 1997, page 75.

“Methodology Mentor: The Need for Software Risk Management Tools”, Charles Martin. **Application Development Trends**, June 1997, page 20.

“Managing Risk of Client/Server Deployment”, Zohar Gilad. **Data Management Review**, May 1996, page 10.

“I/S Management: Reducing Project Risk”, **Enterprise Systems Journal**, March 1995, page 28.

“Risk Analysis: How Good are Your Decisions?”, Steve Pascale, etal. **PM Network**, February 1998, page 25.

“It’s All About Managing Risk”, Ian Hayes and William Ulrich. **Software Magazine**, April 15, 1998, page 12.

Kulik & Lazarus, Inc., *Project Self-Assessment Kit*. Copyright 1997 by Kulik and Lazarus Consulting, Inc.

Keane, Inc., *Project Risk Assessment Model (PRAM)*.

*RISKTRAK*, Risk Services and Technology, 17 Old Nashua Road #6, Amherst, NH 03031-2839.

*Risk Radar*, Software Program Managers Network, 758 South 23<sup>rd</sup> Street, Arlington, VA 22202.