INTRODUCTION
Risk management is the process of identifying and mitigating potential budget, schedule, and technical problems throughout a software development project. The goal of risk management is the avoidance and control of any situation that may impact the project in a negative way. The task components of risk management are assessment, evaluation, and mitigation.

As a discipline, risk management has existed in many industries for decades, but it was not defined for the software industry until the late 1980s. It was then that works by Barry Boehm and Robert Charette brought attention to risk management in response to senior management’s increasing awareness that something had to be done to better control software development efforts. The U.S. Department of Defense, the largest single procurer of software products and software development services, took these works seriously. Phrases such as “characteristics of project operations,” “factors opposing project success,” and “quantitative risk ratings” became common in board rooms when the initiation of software development efforts was discussed. The more complex the effort, the more the terms were used, and the more management demanded concrete evidence the project, once funded, would be able to meet the expectations laid out for it.

In Robert Charette’s book, Software Engineering Risk Analysis and Management, copyrighted in 1989,
the mathematical theories, relationships, formulas, and graphs for implementing risk management are explained in great detail. The mathematics allow risks to be quantified.

The information Charette provides is comprehensive, easy-to-read, and valuable. It is also involved — perhaps too involved — to ensure the implementation of risk management on projects outside of the federal government. Most organizations in the commercial sector do not have the budgets or sufficiently skilled staff members to dedicate to a full-time risk management position, so risk management is never identified as a component of the project. This, of course, is the first risk to the success of a project planned by the organization.

SIMPLIFY THE PROCESS

Rather than ignoring risks on a day-by-day basis and going into crisis mode every time a problem raises its ugly head like a sleepy dragon coming to life, why not use the essential elements of risk management and make them work in an organization? In other words, simplify the risk management process to meet the needs of the organization.

To build a customized risk management process, the basic principles of risk management need to be known and understood. First and foremost, it is important to understand the definition of risk. Risk has been defined as an event having three elements associated with that event: chance, choice, and consequence.

- **Chance** means that there is a probability that the event will occur. For example, if the development of a system relies on software deliveries from one or more outside vendors, then there is a chance that one or more vendors will fail to deliver on time.
- **Choice** means there are alternatives to the event. In the example given for chance, a different vendor could be selected, or the software could be developed in-house, or some work-around technique could be used to get around obstacles caused by a late delivery.
- **Consequence** means that if alternatives are not identified and assessed, there will be a negative impact of some kind on the project. Again, using the example of an outside vendor dependency, if a delay occurs, the schedule will slip and the project will cost more money.

If any one of the three elements of risk is missing in evaluating an event, the event is not a risk. It may be a condition, a situation, or a challenge, but it is not a risk. If there is no chance that the event will occur, then there is no risk. If there is a chance the event will occur but there are no choices associated with the event, it is not a risk. If there is a chance the event will occur and there are alternatives, but there will be no negative impact if the event is left alone, there is no risk.
All three of the elements of an event are needed for the event to be a risk. Keep in mind, the intent of risk management is to reverse Murphy’s Law. Instead of “everything that can go wrong will go wrong,” risk management makes it “anything that could go wrong will be identified and mitigated before it can go wrong.”

**SOURCES OF RISK**

Risks originate from one of three things: events caused by others, events imposed by the organization, or events occurring as acts of nature. Events caused by others can include:

- not getting hardware or software delivered or installed as promised by an outside vendor
- not having the wiring in a building meet specifications for handling the computers
- employee resignations
- customer needs and requirements changes

What about an established vendor, such as Microsoft, Oracle, or Hewlett-Packard, going out of business or deciding not to manufacture a product midway through the project? Is that a risk? It is unlikely that it is, because there would be little to no chance of that happening to an established vendor that has a reputation of supporting multiple computer projects around the world.

What about the organization itself? Can events caused by the organization be a source of risk? Consider an internal reorganization. All organizations experience them, some more frequently than others. The effect of an internal reorganization can be to either increase risk or decrease risk.

Only when the reorganization is at the highest levels, or does not affect a particular project, would it have no effect in terms of risk. This is because in every instance there is a period of adjustment for team members, however short-lived it may be.

An internal reorganization increases risk during a reorganization when the new reporting structure disrupts the flow of work by moving technical personnel from one team to another team, causes an upward learning curve for a new manager or team leader, or changes the scope of responsibilities for individual teams or departments.

An internal reorganization will decrease risk when it improves the flow of communication, provides better leadership, or enhances the natural flow of work effort within the organization.

Besides internal reorganizations, organizations can and often do impose risks to production. Many of these risks can be classified as “lack of” factors that contribute to risks, including:
• Lack of resources. Whether it is time, people, or equipment, when upper management fails to fully support the need for resources, both budget and schedule are put at risk. A classic example of this showed up on many Year 2000 projects when management did not include sufficient dollars on the capital expenditure line to replace all of the desktop computers that needed to be swapped out.

• Lack of information. Whether it is managerial, technological, or marketing in nature, projects suffer when communication is weak, goals are hidden, and people do not clearly understand what is needed or expected. This factor was clearly the demise of one multimedia project that failed to even get off the ground because the decision for what technology to use in developing a multimedia driver was never made. The reason it was not made was that management never clearly conveyed marketshare information with the technical team.

• Lack of training. Whether it is formal classes or on-the-job technical transfers, projects suffer when organizations fail to provide personnel with the type of training needed when it is needed. This happened in many organizations that lost good programmers who felt they were becoming technical dinosaurs as technology moved rapidly from mainframe systems to client/servers and from internal processing to Internet access.

What about organizations dealing with customers who constantly change their directions regarding the project? Does that constitute lack of customer control? Perhaps, but only if customer control is essential to the organization. Most organizations servicing customers accommodate them. In these organizations, when customer directions change, the project plan is changed. There is no risk because the business methods for the organization recognize that their customers may change their minds and procedures are in place to deal with the changes.

Events resulting from acts of nature are circumstantial. For example, there is no risk of a hurricane in Las Vegas; but if the development effort is located in Miami or anywhere in the state of Florida, a hurricane may become a risk. Power outages resulting from major thunderstorms in Chicago during the spring and summer could well be a risk because there is a chance it could happen, there are alternatives for handling an outage situation, and there are definite consequences of dealing with a major power outage if advance preparations are not made. Consider the circumstances of acts of nature such as a fire, flooding, and blizzards and ice storms. What about a heat wave resulting in “brown outs?” Would this be an act of nature to be assessed as risks are identified? Again, it is circumstantial. It certainly would not be a risk in North Dakota; but what about in New York or Georgia? If there is a chance, if there are choices for dealing with the event or compensating for its impact in advance, it is a risk.
ASSESSING RISKS

The responsibility for identifying and avoiding risks belongs to the project manager. While the best way for the manager to ensure that all real and potential risks are identified is to solicit input from every person involved with the project; risk assessment can begin today, this minute, by just starting a list. Exhibit 1 presents a sample risk assessment.

Fold a piece of paper in thirds, create a three-column table in Word, or open Excel, and get started. Label the columns: Events, Probability, and Mitigation. In the first column, list events such as there are too many meetings; too many interruptions; Joe does not come in until 10:30 a.m. every day; the scanning equipment will not be delivered until June, The

<table>
<thead>
<tr>
<th>Event</th>
<th>Probability</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are more programs to be remediated between now and year 2000 than time needed</td>
<td>High</td>
<td>Make certain the inventory is complete. Start triage. Schedule remediation according to priority.</td>
</tr>
<tr>
<td>Limited availability of AS/400 programmers for remediation</td>
<td>High</td>
<td>Extend search for programmers nationally and internationally. Identify tools to support AS/400 remediation. Develop incentives for AS/400 programmers to join team and stay to completion of project.</td>
</tr>
<tr>
<td>Interfaces between internal applications are not defined</td>
<td>High</td>
<td>Create a common definition for interfaces and make all teams aware of it. Designate a special interface team to identify and document all interfaces.</td>
</tr>
<tr>
<td>Desktop hardware replacement is extensive</td>
<td>High</td>
<td>Designate a special team to inventory, assess, and plan all desktop hardware replacements.</td>
</tr>
<tr>
<td>Desktop software needs to be upgraded to compliant versions</td>
<td>High</td>
<td>Create an amendment to the capital expenditure line in the budget and order the upgrades. Develop a plan for installation once the equipment is received. Hire contractors to support the effort as needed.</td>
</tr>
<tr>
<td>Vendor remediation and testing is not completed by the time testing is scheduled to start</td>
<td>High</td>
<td>Develop a contingency plan for all vendor products that are not prepared to provide Year 2000-compliant software by June 1999 (or pick a date).</td>
</tr>
<tr>
<td>Direct interface testing is not scheduled</td>
<td>Medium</td>
<td>Reassess the testing process to determine if the “sneaker net” method of testing with input files captured from external systems is sufficient for testing interfaces. Document any changes to interfaces and schedule them for testing.</td>
</tr>
<tr>
<td>Vacation time may jeopardize the schedule</td>
<td>Medium</td>
<td>Create and publish a vacation policy for all personnel attached to the Year 2000 project. Remember, programmers are people and will need time off. Plan for emergencies by staffing adequately.</td>
</tr>
<tr>
<td>There are only two printers for six projects</td>
<td>Low</td>
<td>Order another printer.</td>
</tr>
<tr>
<td>Software upgrades create user learning curve</td>
<td>Low</td>
<td>Training will be provided to all users who need to learn new software.</td>
</tr>
</tbody>
</table>
Farmer’s Almanac predicts several blizzards this winter. Include everything and anything that is or could soon interfere with meeting the product delivery on time and within budget. Do not be concerned about the value or wording of the event at this point.

Now, solicit input from team members. Create a method for team members to report risks. The more simple the method, the more effective the solicitation. Circulate the piece of paper, send out an e-mail with the Word table or Excel spreadsheet attached.

Later in the process, a user-friendly input form created on an Access database might work better. This approach permits the creation of pull-down value menus that can be used to classify risks by department, type, severity, development phase, submitted by name or initials, and status. It will also permit memo space for entry of a description and a resolution. Reports can easily be generated in any order needed, and a comprehensive history of the project is maintained. Making the risk database available to the team allows a project manager to quickly view the state of the project. It also increases awareness among team members. Additionally, statistical data from Access can be easily imported to Excel to produce graphs and charts for presentations to upper management throughout the course of the project.

The goal right now is to just get people thinking about the things that impact development. Get as much input and as many events listed as possible. Proceed by assuming every event listed poses some risk to the project or organization.

EVALUATING RISKS

While one or more of the formulas and methods for weighting and measuring risks mentioned earlier in this article can be adopted as the benefits of risk management procedures in an organization are implemented, they are not essential to implementing risk management today — this very minute.

What is necessary is to evaluate the list of events. Look at the events in column 1. Then, in the column 2, assign a probability factor. The probability factor will be high if the event is very likely to occur. It will be medium if it is likely to occur but not as likely as high, or if the impact to the efforts are not traumatic. Assign a low probability factor if the event is not apt to happen or if the impact is very low. If anyone lists “the discovery of new alien technology” as an event, cross it off the list along with any other events having a remote likelihood of occurrence.

In most cases, known information will readily dictate what value to assign to the probability factor for an event. In some instances, research may be required. For example, an event that simply states “Microsoft modifications to Java,” is obviously referring to recent court rulings that Microsoft
cannot invent its own Java methods to support MS Explorer to the exclusion of the competition. Still, understanding how this ruling is going to impact product release on a specific project is worth investigating.

If the organization builds tools to support object-oriented development, such as Rationale orSegue Software, Inc., it might mean there is a question as to how to proceed with the development of the various versions currently offered by the company. The decision on how to proceed could have a high impact if it is delayed. If, however, the organization is planning to purchase tools for the development of an Internet store, such as Amazon.com, it would have a lower probability factor because the organization can control the development direction and select tools accordingly. In either case, it is worth questioning the person who listed the event to determine the context in which the event was listed.

Once each of the events has been assigned a probability factor or even before the investigation is fully completed, mitigation can begin.

MITIGATING AND MANAGING RISKS
Mitigation is the process of identifying an alternative method to handle an event, or of eliminating it all together. Begin mitigating all of the events given a high probability factor.

First, look at the event carefully and decide if there is anything that can be done to eliminate or avoid it. In some instances there is nothing an organization can do but grin and bear it. Before the potential of the Year 2000 bug gained reality, losing all electrical power due to a catastrophe fell into this category. Now, contingency plans are being written and practiced at many plants across the nation and around the world.

What about natural disasters, acts of God? Consider a tornado: if the organization is located in Alaska and it is the dead of winter, the event was probably crossed off the event list because it has a negative probability factor of –100. But take the probability of the same event disrupting a project in Oklahoma in the late spring. The event stayed on the list with a high probability. The tornado itself cannot be eliminated, but the disruption can be kept to a minimum by having a disaster recovery plan ready to be put into effect. The development of the disaster recovery plan, if one does not already exist, must be scheduled to mitigate the risk of disruption.

Reassessment
The examples deal with events that may not have even been put on the list. Go back and check the list again. This time, try to think of everything. Add events that were not addressed the first time. Assign probability factors. Start mitigating.
BENEFITS
The benefits of implementing even the simplest of risk management programs should begin to show up immediately. Signs that it is working include:

- There will be fewer surprises in any given workday, resulting in greater productivity for the project manager and all team members.
- There will be a renewed confidence in the team because they will feel more comfortable that management does, in fact, know what is going on.
- Chances of meeting the schedule will be improved because obstacles have been anticipated and dealt with in advance.
- The chance of budget reporting being more accurate will be improved because all possible angles of the project have been accounted for.

Each of these individual benefits lends itself to even greater benefits over the long haul. If turnover has been a problem in the past, expect it to decrease as management gains greater control of the factors that impede the progress of developers and cause frustration. If system down-time has interrupted development and resulted in unplanned overtime more times than desirable, expect upper management to, at a minimum, understand that there is a solution to the budget overruns by doing after-hour maintenance, increasing machine size, or running parallel systems.

Listing these benefits could continue for pages. Each organization will realize unique value in its own problem areas. The point is: this simple process of risk management can make a difference in every organization. Implementing a formal risk management program does not have to make the process difficult or cumbersome. One may want to start slowly. What is key is that one starts the process.

---

Polly Perryman Kuver has more than 19 years of computer experience. As a process engineer, her areas of expertise are national and international software engineering and documentation standards, and quality assurance. She is currently a consultant in the Boston, MA area.