

THE SOFTWARE TESTING & QUALITY ENGINEERING MAGAZINE

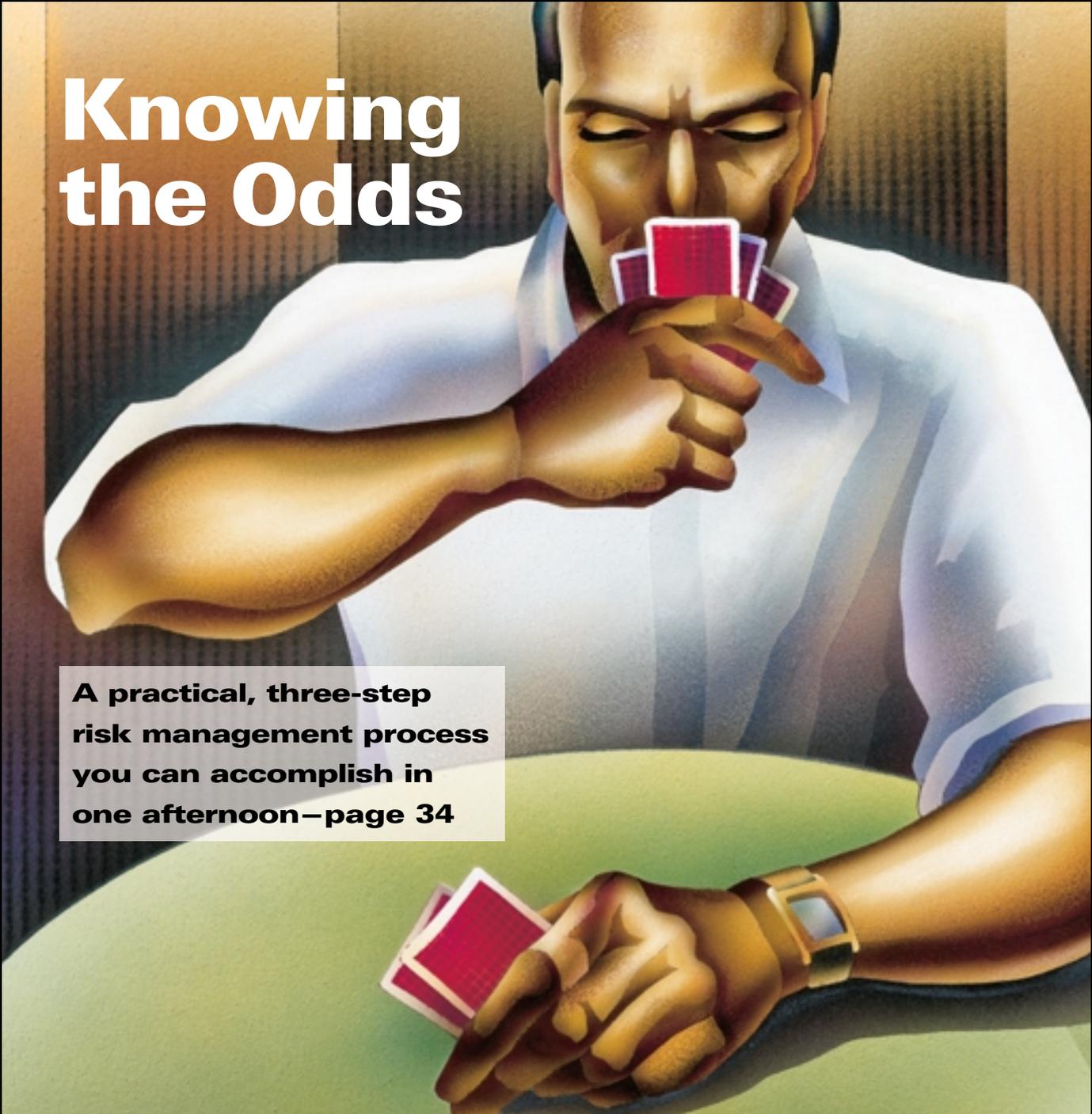
STQE

VOLUME 5, ISSUE 2
MARCH/APRIL 2003

**Turning Metrics Into
Effective Graphs**
page 20

Security Bugs—Exposed
page 26

**Using Action Words
in Model-Based Testing**
page 42



Knowing the Odds

**A practical, three-step
risk management process
you can accomplish in
one afternoon—page 34**



© PELLISART.COM

INFO TO GO

This is the second of a two-part series on risk management. For more background on overcoming resistance to risk management, we encourage you to read Payson Hall's "A Calculated Gamble" in the January/February 2003 issue of STQE.

- Laying a foundation for risk management is a 3-step process consisting of identifying risks, analyzing their potential severity, and selecting appropriate responses.
- When brainstorming with your team, it's important to capture all of the information. It will be sorted later.
- The results of risk analysis should always be documented and reviewed with the team and the sponsor so that risk choices are explicit, conscious decisions.

Knowing the Odds

A practical, three-step risk management process you can accomplish in one afternoon

by Payson Hall

HAVE YOU EVER BEEN ON A PROJECT THAT WENT EXACTLY like the best-case scenario, where nothing went wrong? Neither have I. Bad things can happen to any project; every project is a calculated gamble. Investing a single afternoon focusing on risk identification, analysis, and response can improve the odds of meeting project goals for a typical development effort.

That's right. I will describe a risk analysis process that you can do in just one afternoon. It is simple enough that it is likely to succeed the first time you use it, and inexpensive enough that not much is risked in applying it once just to see if it works for you.

For the purposes of our discussion, we'll define a "typical" project as being six months in duration and having a development team of ten people. Understand that as size, complexity, and the impact of project failure rise, good

It is important to make clear to the team that “negative thinking” is acceptable.

risk management will require an additional investment and more sophisticated techniques. If you are working on a large, complex, high-risk project whose failure will result in loss of life or extreme economic consequences, then what follows will be useful and necessary, but insufficient. My goal is to get you started and to convince you (and your team and your management) that the afternoon invested was worth more than it cost.

The process steps on your afternoon’s agenda are

1. Identify Risks
2. Analyze Potential Severity
3. Select Appropriate Responses

Identify Risks

Identification of potential risks is a team activity. It is also a great excuse for an off-site. If you have the budget, get a hotel room and hide for the afternoon. If funds are tighter, consider having the team to your house for pizza and risk, or finding a conference room in some obscure corner of your building where you can hide. Getting people away from distractions for a few hours is key.

Materials needed to support risk identification should be readily available. You will need

- Your project charter, plans, and assumption list
- A flip chart and easel, some markers, masking tape, and a few packages of yellow sticky notes
- If available, retrospectives from previous similar projects, where *similar* might refer to similar technology, similar applications, or previous projects for this client

Brainstorm The first step is to identify specific potential challenges that your project might face in the future. The outcome of this step will be a list of risks specific to your project. It is important to make clear to the team that “negative thinking” is acceptable as part of this process. Using a list of questions like the

one in the sidebar “List of Risks” will usually help an experienced team generate several dozen serious risk items in less than an hour. Have people write the risk items they identify on yellow sticky notes so you can sort them later.

Review and Consolidate Once the time allotted for brainstorming has elapsed, review the list, looking for ways to tighten it up. A “good” risk item is specific. “Bad things could happen” is not a particularly actionable risk. Even “We could lose a team member” is terribly broad.

For example, if you have a surgical team that consists of two surgeons, two surgical nurses, and one anesthesiologist, the anesthesiologist is a critical resource who does not appear to be backed up. If the anesthesiologist becomes unavailable for some reason, the surgery project may be in more serious trouble than if one of the surgeons or nurses becomes unavailable. You need to be specific.

At the same time, consolidating risks into common themes can also be helpful. For example, the team might identify that the anesthesiologist could

- be late,
- get sick,
- get called away to an emergency,
- be abducted by aliens, or
- die of old age.

You don’t have to list each of those risks separately. The common theme is “The anesthesiologist could be unable to perform his or her duties during surgery.” Address the common risk, and you have addressed many of its constituent parts.

Be gentle as you look for ways to consolidate risk items by cause or effect, or improve the specificity of risks. *It is important that you do not discard risks offered by others.* Useful questions include:

- These two risks seem to have something in common. Is there a way we could restate them?
- How would we know if this happened?
- What would be the effect of this risk occurring?
- What are some specific things that could cause this risk to occur?

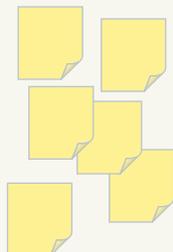
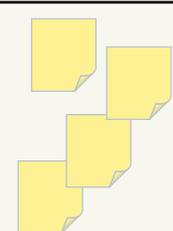
Risk	Impact	Probability	Surprise
	M	H	M
	H	M	L

Figure 1: A risk analysis matrix helps you analyze the potential severity of each risk.

A rich list of risks provides fertile ground for considering possible mitigations.

Make a Chart Once risks have been consolidated, restated, clarified, and expanded, place the resulting clumps of risk sticky notes on the left side of a sheet of flip-chart paper under the heading “Risks” (see Figure 1), and you are ready to begin the next step: analyze potential severity.

Analyze Potential Severity

A list of dozens of risks can be daunting. Most project management texts suggest that you identify the top five or top ten risks, then develop mitigation strategies and contingencies and monitor these risks closely. While this is helpful *in theo-*

ry, in practice it can be difficult to sort the risks cleanly, and there may be simple and inexpensive strategies that could mitigate risks eleven and seventeen before you put them out of your mind. So the next step in the process is intended to provide a basis for crude sorting, while also laying a foundation for thinking about risk mitigation.

Risks are quantified using the risk analysis matrix in Figure 1. Each risk is assessed in terms of

- Impact to the project if the risk occurs
- Probability of the risk occurring
- Surprise (or difficulty of timely detection) of the risk

The **impact score** addresses the question, “If the risk event occurred, what is the impact to the project?” Some risks would be fatal to the project (impact = high), others merely annoying (impact = low), and still others fall somewhere in between. For example, if a major portion of your project involves building an interface to a prototype piece of equipment and only one of those devices exists for your testing, the loss or destruction of that equipment (assuming it cannot be easily replaced) might be a high-impact risk. On the other hand, if you have a small development team in one geographic location and take off-site backups of servers and key documentation on a regular basis, loss of the facility or its contents might have medium impact (if you

List of Risks

As a project manager or team leader, your role is to facilitate the brainstorming session. You can use this list of risk areas and questions to get people thinking, and also to make sure you haven’t missed any major categories of risk. Monitor the group during brainstorming and try to help people feel comfortable participating. Assure that all ideas are captured (even the silly ones). Remember, no filtering during brainstorming. If people are having trouble, ask a few questions (rather than identifying risks yourself) to encourage participation. If people get stuck (including yourself), call a break. (For a downloadable list with examples, go to the StickyNotes at www.stqemagazine.com.)

POTENTIAL RISKS

Failure of specific tasks.

Loss of specific resources (people, equipment, work products, data, facilities, etc.). Loss could mean resources pulled for another project, hit by a truck, or just an extended absence.

Significant schedule overruns for specific tasks (particularly those on the critical path and those which use hard-to-obtain resources).

Late delivery of key components or information.

Failure of key reviews or tests.

Delay of funding.

Incorrect assumptions. Review the assumptions list—an excellent source of risks.

Historical problems with similar tasks.

Technology risks.

High-cost tasks.

EVOCATIVE QUESTIONS

■ Which tasks would be problematic if they were not completed successfully?

- Which resources are we most likely to lose during the project?
- Which resources would be most painful or problematic to lose during the project?

- Which tasks would cause problems if they ran long?
- Which tasks have estimates that are the least stable or predictable?
- Which tasks would cause problems if they were started late?

■ Where do we have high sensitivity to the scheduled receipt of equipment, software, or information?

- Not all test/review tasks are created equally. Which tests or reviews would be most disastrous if they *didn't* detect errors present?
- Which tests or reviews would be most problematic if they *did* detect numerous problems?

■ What funding points have been identified for procurement of hardware, software, or services?

- Which assumptions would prove particularly troublesome if they were incorrect or changed?
- Which assumptions will not be resolved/verified until the last minute?

■ In your experience, what kinds of problems might be expected as work is completed?

- What new technologies are being used, and when will we know that they perform as advertised?
- Are we combining technologies in any novel ways?

- Which tasks consume the most resources?
- Which tasks risk the most resources if they are done incorrectly?
- Which work products represent the highest resource investment?

assume you could get space in a nearby facility and have your hardware environment restored in a few days and that a one- to two-week delay would not be fatal to your project). Finally, if your servers and workstations are relatively standard configurations and backed up nightly, loss of a single server or workstation might be considered a low-impact event (if you assume that you could replace the equipment within 24 hours and would not lose more than one day's work).

The **probability score** speaks to the question, "What is the likelihood of the risk actually occurring during the life of the project?" Some specific risks can be expected to occur during the life of the project (probability = high), others may

be considered remote possibilities (probability = low), and still others fall somewhere in the middle. For instance, if the last two major releases of the operating system shipped over thirty days late, and one of your risks is "The new operating system may arrive thirty days or more late," the probability of that risk would be high. Reasonable people expect that the future will be a lot like the past. In the same way, if you are the biggest client for one of your subcontractors and they have a track record of delivering quality products within two weeks of their committed dates, you might assess the probability of the risk "Subcontractor delivers product more than one week late" as medium. Conversely, although you may have never lost access to your building

and its contents in the past, you are unable to fully control all potential threats to the building. Facilities can be destroyed or made unavailable by fire, flood, earthquake, tornado, vandalism, terrorism, or a nearby chemical spill. The probability may be low, but the risk may still require further consideration.

Surprise is a subtle notion that provides a powerful framework for later mitigation. Surprise refers to the difficulty of *timely* detection of the risk event if it occurs. Surprise answers the question, "If the risk event occurs, do our current plans provide mechanisms to detect the event in time for a meaningful response?" High surprise is a bad thing. Low surprise is preferred. Earthquakes



Watch One Team Analyze Risk

LET'S LISTEN AS A TEAM SPENDS ONE AFTERNOON analyzing risk. We'll concentrate on the risks of their current reliance on a single server as the repository for all of their developed code.

JUAN: We could have a hardware failure on the server.

ELISABETH: The server could be stolen.

MICHAEL: Someone could spill coffee on the server.

JUAN: That *would* cause a hardware failure. It's the same thing.

LEADER: Write all those down on sticky notes. Let's move on.

The team clumps all of these risk sticky notes under the heading "We might lose access to the server or its contents."

LEADER: It might be helpful to identify other common causes of lost access.

Several new ideas get added to the clump, including power spikes, sabotage, accidental erasure, and temperature fluctuations.

LEADER: Okay guys, it's time to score the risks. What is the likelihood that we might lose access to the server contents?

MICHAEL: The specifications on the hard disk say the expected reliability is one hundred thousand hours mean time between failures. That's over ten years and this is only a three-month

project. I think the probability is low.

ELISABETH: The last project I worked on lost two server disks in six months. I think the probability is high.

JUAN: But this is a new server. If we got an uninterruptible power supply, I don't think the risk would be high. It would be more like medium.

LEADER: A UPS might be a great solution, Juan. Make a note of that. Our goal right now isn't solutions—just scoring. Remember: The pessimist wins. Let's make the probability high and move on. We can revisit it later. What about the impact? What is the impact to the project if we lose access to the server contents?

ELISABETH: On our last project, when the disk failed, we lost a week's worth of data. After that, we did nightly back-ups, so that the sysadmin error only cost us a few hours. I'd say low.

JUAN: Wait a minute, though. We haven't specified that *our* server should be backed up daily. That might be a good idea, but right now I think we are on the standard weekly back-up schedule. Losing a week's worth of work could really hurt the effort. I think the impact would be medium to high.

LEADER: Michael?

MICHAEL: I'm not sure. It sure would be a drag to lose a week's work, but it wouldn't be fatal. Medium?

JUAN: How about medium plus?

are generally high-surprise events because they occur without warning. Hurricanes are low(er)-surprise events because there are usually several days of warning before the event occurs.

Again, as an example, if you are building a non-trivial interface to system X that will not exist for testing until just before your software goes into production, the risk “Interface issues are detected with system X during testing” might be considered a high-surprise event. Similarly, imagine that you have a distinct test environment set up to enable full testing of all development tool maintenance releases and upgrades. Your policy requires that your current development environment be recompiled and regression tested successfully in the testing environment before the

tools are made available in your development environment. In that case, the risk “Upgrades or maintenance to development tools introduce anomalies into development environment” might be deemed medium-surprise. On the other end of the spectrum, if you are confident about the predicted usage patterns of your software system and have plans to conduct a full-scale performance test on comparable hardware early in your project life cycle, the risk “System performance is unacceptable under predicted load” might be deemed low-surprise. This is especially true if early detection will give you ample opportunity to either correct the problem or cancel the project before further investment. Note: The impact of the risk might be huge (cancellation), but the early op-

portunity to assess the outcome and respond would equate to low surprise.

If these scores seem subjective, they are. After all, what *is* the four-decimal-point probability of your chief architect becoming unavailable to your project for more than five days during the next twenty-three weeks? You don’t know for sure, I don’t know for sure, she doesn’t know for sure. If she is well paid, healthy, happy, has a healthy family, doesn’t engage in extreme sports, and is unlikely to get pulled for a higher-priority project, let’s just say it is a low-probability event and leave it at that. The goal isn’t precision—it’s triage. If your team insists, you can invent more refined scores like *H-* or *L+*, but don’t spin your wheels trying to get too precise. Once the matrix has been

LEADER: Medium plus it is. What about surprise? Will we have adequate warning before we lose access?

ELISABETH: Do you mean that warning message that pops up and says, “This is the server. I’m planning to fail tomorrow at 3:00. Now would be a good time to back up your stuff?”

MICHAEL: Now *that’s* a useful warning message! I guess the surprise would be high, until we get smarter devices.

After this exchange, the risk analysis matrix for this particular risk would look like this:

Risk: We might lose access to the server contents.

Probability: H

Impact: M+

Surprise: H

Next, the team discusses ways to mitigate the risks they have listed.

LEADER: Okay gang, let’s revisit losing our server. How can we reduce the probability of server content loss?

JUAN: Is this where the UPS would come in?

LEADER: Yes. Let’s add “obtain and install UPS” to the to-do list. What else?

MICHAEL: What if we have our server placed on the nightly back-up rotation?

LEADER: That’s a great idea, but that ad-

dresses reducing the impact, not the probability. Let’s make a note of the idea for later. What else can we do to reduce the probability?

JUAN: We identified environmental risks, such as temperature and moisture.

Maybe we should move our server to a more controlled environment or outsource it?

LEADER: Those are good ideas, but I’ll need to discuss them with the sponsor before we incur those costs. Let’s put them on my “discuss with sponsor” list.

MICHAEL: We could inspect the server area, checking the ventilation and such. We could also make sure that it isn’t in a high-traffic area or an area accessible to the public.

LEADER: All good ideas. I’ll add them to the to-do list. If we do all this, what would the probability of losing access to the server contents be?

ELISABETH: I guess medium, *if* we do all that stuff.

LEADER: Good. Let’s move on to impact. How can we minimize the impact of losing access to the server contents?

MICHAEL: Nightly back-ups.

JUAN: And take the tapes off-site.

LEADER: Sounds good to me. The revised score?

ELISABETH: Losing a full day’s work and email would be a hassle, particularly as we are refining the requirements and design. I think the impact would still be painful. Maybe medium minus?

JUAN: What if we set up disk mirroring for the server disk? Now can we sell you on low impact, Liz?

ELISABETH: *After* you add “Install Disk Mirroring” to the to-do list.

LEADER: The to-do list has been duly modified. Impact changed to low. What about Surprise?

JUAN: It’s still high. There are no warning messages that say the disk is going to fail.

MICHAEL: Actually, most disk mechanisms don’t fail all at once; they fail gradually over time. I could run weekly, low-level diagnostics on the server disk to get early warning of trouble.

ELISABETH: Please tell me you will run them *after* the nightly back-up!

LEADER: If we add weekly diagnostics on the server after the nightly back-up, what would the surprise factor be then?

ELISABETH: What do you think, medium?

JUAN: Okay, although I still think the warning message was a good idea.

The goal of this process was to identify the low-hanging fruit, the simple steps that can be taken to reduce the probability, impact, and surprise of risks identified by the project team. The result is that the project benefits from Benjamin Franklin’s adage: “An ounce of prevention is worth a pound of cure.”

How to Rate Impact, Probability, and Surprise

SCORING FACTOR	(H)IGH	(M)EDIUM	(L)OW
Impact	The schedule, resource, or scope impact of a risk will likely result in project failure or substantial renegotiation and redefinition of project goals.	The project is still capable of qualified success, but it will be difficult to recover fully; several medium-impact risks in concert can doom a project.	Workarounds are obvious, the schedule impact is minor, and the cost is minimal.
Probability	Risk items are reasonably expected to happen. You would appear naive if you acted surprised when they occurred.	Risk items are clearly possible during the project period, but don't seem likely.	Risk items seem very unlikely, though not impossible.
Surprise	Risk items are not detected until it is too late. The full force of the risk can be expected. High-surprise risks would "blind-side" a project.	Risks have mechanisms established to detect problems early enough to provide some opportunity to avoid the brunt of the event. Medium-surprise risks usually provide some warning.	Events are seen coming from miles away. The impact may still be extreme, but there would be time to react.

filled in, you have visibility on risks and you can begin to select appropriate responses for the risks identified.

Here's a key idea during the initial scoring process: Don't vote—let the most pessimistic team member win. People tend to be sensitized to issues that have come up for them in the past. Rather than talk them out of what seem like ex-

ceptions, remedial actions, or prevention options for addressing the risks. When preventions, remedies, or improved detection mechanisms are identified, the team must assess the feasibility of modifying the project plans to integrate these mitigating actions. This process may involve minor changes to task descriptions, revision or creation of project policies, changes in staffing, changes in task sequence, or sub-

stantial changes to the overall project approach. Within the schedule, scope, and resource boundaries established in the project charter, you and your team might elect to modify the plan to address risks.

ion, and then build upon your earlier successes and failures. The activities just described will help build a list of risks that can be "sorted" in crude fashion based upon the risk scores remaining after the team's initial mitigation review. Then, this list can be reviewed with the project sponsor.

Good gamblers don't rely on luck: they know their opponents and they know the odds. You can never eliminate all risk from a project. You *can* encourage informed choices, tradeoffs, and open discussion of potential risks and problems. With this practical risk-management process, you'll discover ways you can inoculate your project against many risks, and cushion the blows from others. You will be able to drive defensively in hazardous areas and monitor potential dangers as you approach them. If your project is determined to fail, try to find a new and creative way to do it. Don't fail for a reason you could have reasonably anticipated, defended against, or detected before it was too late. **STQE**

You can never eliminate all risk from a project.

treme scores, capture the scores and move on. Rationale for scores can be discussed as part of exploring mitigation.

Select Appropriate Responses

The risk analysis matrix provides a framework for a discussion about responses to risk. After preliminary scoring is complete, review each risk with the team and brainstorm ways to lower the individual risk scores. This can be accomplished through

- Impact reduction measures that decrease the resulting harm if a risk event does occur
- Preventative measures that reduce the likelihood of risk event occurrence
- Improved early detection mechanisms to increase the ability to detect risk events in a more timely fashion

Focusing the team on the different aspects of risks can help members identify differ-

ences and then build upon your earlier successes and failures. The activities just described will help build a list of risks that can be "sorted" in crude fashion based upon the risk scores remaining after the team's initial mitigation review. Then, this list can be reviewed with the project sponsor.

The End of the Afternoon and the Path Forward

The afternoon exercise described above involves getting a capable risk assessment team together to identify, analyze, and mitigate risks. The results are typically not only a to-do list of items that will help manage risk, but a clearer idea of which risks remain and where the team should focus its attention.

Risk assessment should occur during planning, and it should be revisited whenever there is a substantive change in the project definition, team, approach, or context that alters the risk profile of the project. Revisiting risks periodically with the team and adding tasks to plans to monitor specific risks is part of proactively managing risk. The way to get better at risk management is to begin doing it in some limited fash-

Payson Hall is a consulting systems engineer, project management consultant, instructor, and speaker from Catalysis Group, Inc. He has performed and consulted on a variety of hardware and software systems projects during his twenty-five-year professional career. Reach Payson at payson@catalysisgroup.com.

STICKYNOTES

For more on the following topics go to www.stqemagazine.com

- Downloadable risk and ratings lists

StickyNote 1

List of Risks

As a project manager or team leader, your role is to facilitate the brainstorming session. You can use this list of risk areas and questions to get people thinking and also to make sure you haven't missed any major categories of risk. Monitor the group during the brainstorm and try to help people feel comfortable participating. Assure that all ideas are captured (even the silly ones). Remember, no filtering during brainstorming. If people are having trouble, ask a few questions (rather than identifying risks yourself) to encourage participation. If people get stuck (or you get stuck) call a break.

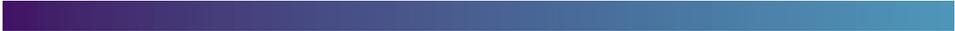
POTENTIAL RISKS	EVOCATIVE QUESTIONS	EXAMPLES
Failure of specific tasks	<ul style="list-style-type: none"> Which tasks would give us grief if they were not completed successfully? 	<ul style="list-style-type: none"> Requirements Gathering Interface specification Critical component design
Loss of specific resources (people, equipment, work products, data, facilities). Loss could mean "pulled for another project," "hit by a truck" or just an extended absence	<ul style="list-style-type: none"> Which resources are we most likely to lose during the project? Which resources would be most painful or problematic to lose during the project? 	<ul style="list-style-type: none"> Computers, Key equipment Buildings, Network access Paper files, Electronic Files Personnel: Architect, Lead designers, Lead testers, Configuration manager, Subject matter experts, Project Manager Access to sponsor or key users
Significant schedule overruns for specific tasks (particularly those on the critical path and those which use hard to obtain resources)	<ul style="list-style-type: none"> Which tasks would give us grief if they ran long? Which tasks have estimates that are the least stable or predictable? Which tasks would cause problems if they started late? 	<ul style="list-style-type: none"> Key document reviews Short testing cycles Short review cycles Swapping in new equipment Integration points for different parts of the system File conversions
Late delivery of key components or information	<ul style="list-style-type: none"> Where do we have high sensitivity to the scheduled receipt of equipment, software, or information? 	<ul style="list-style-type: none"> Receipt of new hardware or software Receipt or finalization of interface specs Completion of key portions of design or requirements documentation Finalization of applicable standards
Failure of key reviews or tests	<ul style="list-style-type: none"> Not all test/review tasks are created equally. Which tests or reviews would be most disastrous if they DIDN'T detect errors present? Which tests or reviews would be most problematic if they DID detect numerous problems? 	<ul style="list-style-type: none"> Integration tests scheduled for late in the development process Tests of updates to the operating system software or development tools Tests of new hardware Reviews of interface specifications Performance or reliability tests scheduled late in the development cycle
Delay of funding	<ul style="list-style-type: none"> What funding points have been identified for procurement of hardware, software, or services? 	
Incorrect assumptions. Review the assumptions list — an excellent source of risks	<ul style="list-style-type: none"> Which assumptions would prove particularly troublesome if they were incorrect or changed? Which assumptions will not be resolved/verified until the last minute? 	<ul style="list-style-type: none"> Subcontractors will deliver a quality product on time Functionality required will be delivered with the next version of the operating system scheduled for release next May
Historical problems with similar tasks	<ul style="list-style-type: none"> In your experience, what kinds of problems might we expect as we do this work? 	<p>What issues have arisen in the past working with this:</p> <ul style="list-style-type: none"> User? Sponsor? Development team? Vendor? Subcontractor? Technology? Application Domain? Hardware?
Technology Risks	<ul style="list-style-type: none"> What new technologies are being used and when will we know that they perform as advertised? Are we combining technologies in any novel ways? 	
High Cost Tasks	<ul style="list-style-type: none"> Which tasks consume the most resources? Which tasks risk the most resources if they are done incorrectly? Which work products represent the highest resource investment? 	

StickyNote 2

How to Rate the Impact, Probability, and Surprise Factors

SCORING FACTOR	(H)IGH	(M)EDIUM	(L)OW
Impact	<p>The schedule, resource, or scope impact of a risk would likely result in project failure or substantial re-negotiation and re-definition of project goals. <i>Example:</i> A major portion of your project involves building an interface to a prototype piece of equipment and only one of those devices exists for your testing. It is difficult to replace. Loss or destruction of that equipment: H</p>	<p>The project might still be capable of qualified success, but it will be difficult to recover fully; several medium-impact risks in concert can doom a project. <i>Example:</i> You have a small development team in one geographic location and make off-site backups of servers and key documentation regularly. You could get space in a nearby facility and have your hardware environment restored in a few days. A one-two week delay would not be fatal to your project. Loss of facility or contents: M</p>	<p>Workarounds are obvious, the schedule impact is minor, and the cost is minimal. <i>Example:</i> Your workstations are standard configurations and backed up nightly. You could replace the equipment within 24 hours and would not lose more than one day's work for one team member. Loss of single workstation: L</p>
Probability	<p>Risk items we might reasonably expect to happen. You would appear naive if you acted surprised when they occurred. <i>Example:</i> The last two major releases of your operating system shipped over 30 days late and one of your risks is "The new operating system (OS) may arrive more than 30 days late." Reasonable people expect that the future will be a lot like the past. Probability of late OS: H</p>	<p>Risk items that are clearly possible during the project period, but don't seem likely. <i>Example:</i> You are the biggest client for one of your subcontractors and they have a track record of delivering quality products within 2 weeks of their committed dates. Probability that subcontractor delivers product more than one week late: M</p>	<p>Risk items that seem very unlikely, though not impossible. <i>Example:</i> You may have never lost access to your building and its contents in the past, but you are unable to fully control all potential threats to the building. Facilities can be destroyed or made unavailable by fire, flood, earthquake, tornado, vandalism, terrorism, or nearby chemical spill. Probability of loss: L</p>
Surprise	<p>Risk items that will not be detected until it is too late. The full force of the risk can be expected. High surprise risks "blind-side" the project. <i>Example:</i> You are building a non-trivial interface to a system X that will not exist for testing until just before your software goes into production. You won't know whether or not system X has interface issues until very late in the game. Surprise: H</p>	<p>Risks that have mechanisms established to detect problems early enough to provide some opportunity to avoid the brunt of the event. Medium surprise risks usually provide some warning. <i>Example:</i> You have a distinct test environment set up to enable full testing of all development tool maintenance releases and upgrades, and your policy requires that your current development environment be recompiled and regression tested successfully in the testing environment before the tools are made available in your development environment. Surprise factor if upgrades or maintenance to development tools introduce anomalies into development environment: M</p>	<p>Events that will be seen coming from miles away. The impact may still be extreme, but there will be time to react. <i>Example:</i> You are confident about the predicted usage patterns of your system and have plans to conduct a full-scale performance test on comparable hardware early in your project life cycle. You are confident that the early performance test gives you ample opportunity to either correct problems or cancel the project before further investment. Impact is huge, but because of the ample notice, the surprise factor if system performance is unacceptable under predicted load: L</p>

Notes

CATALYSIS

GROUP
MANAGEMENT & SYSTEMS CONSULTANTS

(916) 929-3629
www.catalysisgroup.com