Risk Management Q&A

1. How are project risks different from technical risks?

   Project risks threaten the project plan, if they become real the schedule may slip or the cost will increase. Technical risks threaten the product quality or timeliness, if they become real implementation becomes more difficult or impossible.

2. Describe the process of building a risk table.

   Project teams begin by listing all risks. Each risk is categorized by type and its probability is estimated. The impact value of each risk is assessed. Risk probability and impact are used to sort the table. Risks are then classified as high impact or low impact by defining a "cutoff" line. High impact risks (those above the line) receive management attention.

3. List three issues that must be dealt with in an effective strategy for dealing with risk.

   Risk avoidance, risk monitoring, risk management & contingency planning

4. Describe all activities that must occur in order to produce a Risk Mitigation, Monitoring, and Management Plan.

   Risk Identification - determine the risks that are appropriate
   Risk Projection - determine the likelihood that each risk will occur and the damage likely to occur
   Risk Mitigation - figuring out strategies to avoid the risks
   Risk Management and Contingency Planning - assuming each risk becomes a reality determine ways to limit their impact

28.1. Provide five examples from other fields that illustrate the problems associated with a reactive risk strategy.

Reactive risk management occur ‘once the horse has left the barn.’ A few examples: putting a stop sign at a dangerous corner only after a fatal accident has occurred; fixing a pothole only after the city has been sued by an angry motorist. In essence, we react instead of planning.

28.2. Describe the difference between “known risks” and “predictable risks.”
Known risks are those that are determining through careful evaluation of the project and technology. Predictable risks are extrapolated from past experience.

28.4. You've been asked to build software to support a low-cost video editing system. The system accepts digital video as input, stores the video on disk, and then allows the user to do a wide range of edits to the digitized video. The result can then be output to DVD or other media. Do a small amount of research on systems of this type and then make a list of technology risks that you would face as you begin a project of this type.

Technology risks:

- Rapid changes in digital format for video data
- Changing compression algorithms and format
- Rapid changes in processing power and bus architectures
- Rapid changes in video input modes (e.g., via internet, direct from camera, across LAN, from analog tape, from DAT),

All of the above represent technology risk for the project

28.5. You're the project manager for a major software company. You've been asked to lead a team that's developing "next generation" word-processing software. Create a risk table for the project.
28.6. Describe the difference between risk components and risk drivers.

Risk components indicate the four areas of impact that will be affected by risk. That is, risk can impact performance, cost, support, or schedule. Risk drivers are the risks that will have a focused impact on the risk components. For example, some risks will have an affect on schedule; other risks might drive the performance component.

28.8. Develop a risk monitoring strategy and specific risk monitoring activities for three of the risks noted in Figure 28.2. Be sure to identify the factors that you'll be monitoring to determine whether the risk is becoming more or less likely.
28.9. Develop a risk management strategy and specific risk management activities for three of the risks noted in Figure 28.2.
28.10. Attempt to refine three of the risks noted in Figure 28.2, and then create risk information sheets for each.

Risk: from table — "Lack of training on tools"

Mitigation: (1) Develop a training schedule for all software staff that is "just-in-time." That is, training will be provided just before the tool is required for use. (2) Have one or two experts on staff for each tool. These people will be available to mentor others in the use of the tool and answer questions.

Monitoring: (1) Log number of hour's tools is being used. (2) Debrief staff to determine how tools are perceived; whether frustration is setting in; (3) examine work products created using tools for quality; (4) determine time required to create work products using tools vs. manual approach—look for anomalies.

Management: Assumes that tools are not working. Determine reasons why. If staff is untrained, then provide one-to-one mentoring/training using staff experts and vendor trainers (budget for this contingency). If training is OK but tools don't work, then consider alternative work product generation approaches using a semi-automated approach, e.g., word processors and graphical tool and a stripped down version of required models.

28.11. Represent three of the risks noted in Figure 28.2 using a CTC format.

Given that the size estimate be significantly lower than the size of the actual system being built then there is a concern that (possibly) only 60% of the project will be completed within the time allocated for the completion of the project.

28.12. Recompute the risk exposure discussed in Section 28.4.2 when cost/LOC is $16 and the probability is 60 percent.

Cost = 18 components x 100 LOC/Component x $16 / LOC = $28,800

RE = P x C = .6 x $28,800 = $17,280

28.13. Can you think of a situation in which a high-probability, high-impact risk would not be considered as part of your RMMM plan?

If a risk is high probability, high impact, but the project team cannot do anything to mitigate, monitor, or manage it; it should not appear in the risk table. For example, if the company goes out of business in the middle of the project, the impact is catastrophic. Assume the probability of this is high, given outside business pressures. The software project team will likely have no control over the outcome.

28.14. Describe five software application areas in which software safety and hazard analysis would be a major concern.

Any application area in which human life can be affected by defects is a candidate: medical equipment, avionics, power plant control (especially nuclear), automobile control systems, and radar. In addition, systems that are involved in national security and systems that facilitate major economic transactions are also candidates.