CSC444 Software Engineering I Fall 2002

Assignment 1: risk management

last updated: Sept 9, 2002

Content

The assignment is to produce a risk management plan for your team project. The plan should cover all three phases of the project, and should address financial, managerial and technical risks. Your risk management plan should have three parts, as follows:

1) A list of your top ten risks. These should be placed in order, with your biggest risk first—and don't forget to describe how you ranked them. For each risk, describe:
   - what the risk is
   - a mitigation strategy for the risk
   - a contingency plan for the risk
   - how you will know when to invoke the contingency plan.

2) A description of the process you will use for managing risk. This can be relatively brief (less than one page of text), but should be detailed enough so that each member of the team understands his/her role in managing risk. For example, how will your team monitor risk? What process will you use for deciding when to invoke a contingency plan? How will you handle emergencies? Will individual members of the team be authorized to carry out parts of your risk management strategy, or will the whole team need to meet and agree each action? How often will you update your list of top ten risks?

3) To help you manage risks, you need to take regular measurements of the status of your project. Choose a suitable set of project metrics that you will collect during your project, to help you monitor risk. Describe five of these metrics in detail, including:
   - what you think it might tell you;
   - whether it is a measure of your *product*, or a measure of the development *process*;
   - how frequently you plan to collect the data;
   - how much effort you think it will take to collect (e.g. in minutes per week);
   - whether the method for making the measurements is algorithmic or subjective;
   - whether the scale used for the metric is nominal, ordinal, interval, or ratio.

Background information

To help you identify, describe and rank risks, you may find the following helpful.

- A *Risk* is a possible future undesirable outcome. For each risk, the *Risk Exposure* is defined as the probability of the undesirable outcome times the size of the loss involved.
- *Risk Mitigation* is the process of reducing risk exposure, either by decreasing the probability of the risk occurring, or by finding ways to reduce the possible impact if it does occur.
- A *Contingency Plan* is a backup plan for use in case the mitigation strategy is ineffective, or only partially effective. It usually describes emergency measures to be used if the undesirable outcome still occurs despite all attempts to prevent it.

Because probabilities are often hard to estimate precisely in the early project planning phases, many projects don't calculate risk exposure explicitly, but rather use a simple scale to compare risks. For example, in its manned spaceflight program, NASA uses a five point scale for assessing loss, in decreasing order of severity: Loss of Human life, Loss of spacecraft, Loss of Mission, Degraded Mission, Minor inconvenience. Loss of mission means that none of the goals of the mission were accomplished, but the spacecraft and crew were safely recovered. Apollo 13 is an example of this

kind of outcome. This type of scale can be combined with a scale for likelihood, to define a number of levels of importance for risks:

		Likelihood of Occurrence		
		Very likely	**Possible**	**Unlikely**
Undesirable outcome	**(5) Loss of Life**	Catastrophic	Catastrophic	Severe
	(4) Loss of Spacecraft	Catastrophic	Severe	Severe
	(3) Loss of Mission	Severe	Severe	High
	(2) Degraded Mission	High	Moderate	Low
	(1) Inconvenience	Moderate	Low	Low

You could apply a similar scheme to your projects, although you would have to adapt the 5-point scale for assessing loss, because there are no human lives or spacecraft at stake in your projects (I hope). However, if you imagine the worst possible outcome (failing the course? not having a project to submit?) as your highest loss, and then define some decreasing levels below it, you can proceed from there. You also need to think carefully about how each square in the matrix should be labeled, as these give you the rankings for comparing risks.

You should also consult the standard software engineering textbooks for hints about likely risks during a software project. In particular, Boehm produced a paper surveying a large number of software projects in industry, and drew up a list of the top ten most common risk factors. It is reproduced on page 192 of van Vliet.

For an introduction to software measurement, read sections 6.1 and 6.8 of van Vliet. *Metrics* are specific items that can be measured to answer questions about a software development project. A metric may be:

- algorithmic—if it does not depend on the viewpoint of the person or machine making the measurement
- subjective—if it involves some subjective judgement, and hence may vary depending on who is doing the measuring

Each metric will have a scale of units associated with it, which may be one of the following:

Nominal—A nominal scale is an unordered set of named categories, such that the only comparison that makes sense is equality.

Ordinal—An ordinal scale is an ordered set of categories, such that tests of relative size (‘greater than’, ‘less than’) make sense. For example, each of the scales in the table of risk categories above is an ordinal scale: a 5-point scale for outcome, a 3-point scale for likelihood, and a 5-point scale (from low to catastrophic) for risk importance.

Interval—An interval scale is an ordered scale where the intervals between the points on the scale are constant, so that addition and subtraction make sense. For example, temperature measured in centigrade: we can add and subtract temperatures, but it does not make sense to multiply them (i.e. 40˚C is *not* twice as hot as 20˚C)

Ratio—A ratio scale is an ordered scale where the intervals between points on the scale are constant, and there is an absolute zero, so that multiplication and division make sense. For example, temperature measured in Kelvin (for which it does make sense to say that 40˚K really is twice as hot at 20˚K).

Marking scheme

Listed below are some of the things your TA’s will look for when marking assignment 1. Use this list to check your work before you hand it in!

Part 1:

- Did they give ten plausible-sounding risks?
- Are the risks described clearly enough so that you understand what the risk is? And are the risks suitably specific rather than vague and general (e.g. "not enough time" is too vague).
- Do the risks they list cover different types of risk: technical risks (e.g. quality of their product, etc) financial risks (e.g. specific problems with resources, etc) managerial risks (project management issues)?
- Do their risks cover the whole term? (i.e. there are some risks that address the later phases of the project?)
- Did they sort the risks in order of priority?
- Did they explain exactly how they prioritized them (e.g. by computing Risk Exposure as a number, or by using a risk matrix, or by having their own tailored scale, etc), and is the method they used appropriate?

- Did they give a (plausible) mitigation plan for all (or most) of the risks?
- Did they give a (plausible) contingency plan for at least some of the risks, and do the contingency plans have some indication of when to invoke them?

Part 2:

- Did they describe their process for monitoring risk (i.e. when will they re-assess their top ten risks, and how will they do this)?
- Did they describe their decision-making process for invoking contingency plans and handling emergencies and is the process effective?
- Is the risk management process described clearly enough so that each member of the team knows what they need to do about risk, and when and how they will do it?
- Does the process for managing risk make sense in relation to their top ten risks? Will problems be noticed in time, will action be taken in time, etc.?

Part 3:

- Did they clearly describe five metrics? It should be clear from each metric precisely what is being measured. E.g. "maintainability over time" is not a metric, because maintainability is not directly measurable.
- Did they describe why they chose this particular set of five metrics, and are their choices sensible? (For example, will measuring these five things give them some reasonable insights into how the project is going? Did they relate them in some way to high level goals? Etc.)
- Is each metric properly defined? Did they provide an appropriate scale and correctly say whether each metric is nominal, ordinal, interval or ratio?
- Did they provide an appropriate frequency of collection for each metric (e.g. daily, weekly, monthly, etc)
- Did they correctly identify whether collection of the metric is subjective (depends on the viewpoint of the person collecting it) or algorithmic (any person collecting the data should end up with the same numbers)
- Did they give a sensible estimate of how much effort each metric would take to collect?
- Did they correctly identify whether each metric is a product or a process metric?
- On balance, is the set of metrics realistic? I.e. will they really collect them all throughout the term, and will collecting them do them any good as far as managing the project is concerned?