CHAPTER 5

A Look at Risk from Classical Project Management

"By failing to prepare, you are preparing to fail."

Ben Franklin

Chapter Purpose

As an Agile Scrum practitioner and coach,
I want to identify and share a part of Classical Project Management
So that Agile practitioners can become even more effective.

It amazes me that the role of risk seems not to be a main concern in Agile Scrum. The reason AgileScrumTeams seem to spend so little time on risk is that Agile Scrum virtually addresses risk by having demos, limiting the duration of time activities can be worked on (iterations) before Product Owners evaluate results, and doing risky User Stories first. Realistically, unless the team is making a concerted effort to address risk, unanticipated events will likely occur more often, and with greater impact. Below, please find a quick introduction to Risk should you choose to adopt risk management in your day-to-day AgileScrumTeam efforts.

Introduction to Risk Management

Risk is the prospect that there could be a difference between what is hoped for and what actually happens. The outcome could be either more negative than projected, or positive. As a practical matter, negative risks tend to get more attention. *The main idea is that you want a plan in place as soon as a potential event is uncovered,* so that should the event manifest itself you are more able to successfully respond to it.

One question is where to store this information related to Risk. Storing risk information in the ALCM is a logical place. I would expect that an ALCM allows for easy access to risks and related metadata as if the risks related to a single User Story, and, the ALCM should allow for entire list of risks so they can be viewed at a project level.

The idea of storing risks and related data on one place is nothing new; in classical project management, they call it a Risk Register.

To continue, there are valuable benefits from assessing risks in your project. For example:

- If you do a good job at risk planning, you will be more prepared than if you did nothing.
- If something comes up out of nowhere and there is a formal investigation, you can point to your formal processes and how effectively you planned, despite the result.
- Working with risk can help teach the people in your organization critical thinking and value-based reasoning.
- This is a good way for teams to learn collaboration, and learn more about their own applications as they start to understand process vulnerabilities, and address them.

Here is a process that has worked for me to address Risk:

Input:

- Any assumptions relating to the project or specific User Stories
- All User Stories in the User Story backlog that will likely get worked on
- Feedback from expert consultation
- History from previous, similar efforts
- When available, any pertinent company records
- Gut feel/intuition

Process:

1. Create a list of known risk events. There are several methods to do this:

   1.1 *Basic Method*: Leverage the inputs to identify Risks that are obvious to the AgileScrumTeam.

1.2 *Brain storming*: Brain storming is a well-documented way for team members to collaborate. This is similar to crowd sourcing.

1.3 *Examining the infrastructure with respect to:*

1.3.1 The current architecture

1.3.2 *How programs interact with each other with in the context of the application*

1.3.3 *Inter-relationships with other applications*

1.3.4 *Ability to discover defects and react to them (Detectability)*

1.3.5 *How information is transmitted and securely stored*

1.3.6 *Etc.*

1.4 *Modified Fishbone* (This assumes that you are familiar with fishbone. If not, this is well spelled out on the web.)

As a risk-assessment tactic, a modified fishbone can be used to assist in understanding the terrain and identifying potential issues well before the code is written. Pretend that when you go into production, and then the deployment was a "total failure." The words "Total failure" is entered in the head the fish. Then the team, with a little imagination, and a few assumptions, is asked to do the Fishbone process as if a real crisis happened. Risks should be captured by a scribe.

2. Once risks are detected, and then entered into the ALCM, here are some examples of metadata that can be included as metadata for risks when described on the Risk Log. Immediately following the description of the metadata will be an example based on the risk potential of drilling a hole into electrical wires that are inside of the walls we are putting dry wall on. These examples will be within brackets and also in italics:

2.1 Impact 1–5: 5 = highest impact *{This is potentially life threatening, therefore an impact of 5 seems appropriate}*

2.2 Probability 1–5: 5= highest impact *{this seems to rarely happen as dry wall installers know to watch out for this so a probability of 2 will be assigned to it}*

2.3 Priority (Scale 1–25: Impact multiplied by Probability) *{an impact of 5 multiplied by a probability of 2 gives us a priority of "10"}*

2.4 If "scale" is greater than your risk tolerance level:

2.4.1 then who "owns" it ("X" is selected by the organization based on their level of risk aversion) *{I would assign the activity of NOT drilling into electrical wires to the dry wall installers}*

2.4.2 Quantitative assessment of risk (e.g., NPV/EMV) *{Though not an NPV analysis, the cost could easily be the cost of covering law suits by people who could get hurt in a potential fire caused by drilling electrical wires. Another cost is the cost of potentially rebuilding the home from scratch.}*

2.4.3 Qualitative assessment of risk *{If workers are hurt, it could take a while to find competent dry wall people to replace them.}*

2.4.4 Trigger event(s) {A trigger event is someone drilling a hole into the dry wall to affix it to the wall and accidentally drilling into electrical wires}

2.4.5 Warning signs *{Some warning signs can include a pop of a circuit breaker, a smoke smell, etc.}*

2.4.6 How to monitor for a risk event *{One could take pictures of the area before drywall is applied and confirm no drilling takes place near wires within the walls.}*

2.4.7 Planned response:

2.4.7.1 Transfer: like insurance, transfer the risk to someone else (realistically, this is very difficult to do in an IT area) *{Buying insurance to protect from workers suing and potential damage to the home would be a good example of transferring risk to an insurance company.}*

2.4.7.2 Avoid: Once the trigger events for a risk are observed, identify how to make those trigger events never take place, or reduce the chance of them occurring *{As mentioned above, pictures can be taken as to where wires are hiding in walls. Not drilling where known wires are should reduce the probability of an adverse outcome.}*

2.4.7.3 Accept the risk as in just let it happen (be especially sure to document this type of risk response, and share your findings with your executive stakeholders for input and approval). *{Though a very bad idea, workers could just ignore the risk and drill away. Again, this would be a very bad idea.}*

2.4.7.4 Mitigating is actually implementing a plan to address a risk (what is nice about this is you actually address the risk head on. But keep an eye on any actual backup process as they tend to decay with time). *{On the day that drywall is put up, close visual inspection can take place to identify the location of wires. Also, sensitive metal detectors could be used to find any hidden wires. All information would be supplied to the dry wall workers. Also, several fire extinguishers are placed near where the dry wall workers will be working. Also, circuit breakers could be tested to make sure they would pop if danger was detected. Giving classes to the drywall installers on safety procedures could also prove helpful. Or, walls could be wired AFTER the drywall is up.}*

2.4.8 What risks are associated with making this change? *{Addressing a risk will likely cause other risks. In this case, trained drywall specialists may resent being told what to do.}*

2.4.9 What stakeholders need to know about this possibility, and if it takes place, who needs to be notified. *{The drywallers need to be made aware of this possibility; so if it happens, they are better able to address the situation. Also, if smoke is smelled, the calling fire fighters to the scene may be appropriate.}*

(*The above was adopted from a previous work of the author, © 2013, and is used with permission.*)

Output:

1. The filled-out risk register.
2. User Stories that are coupled with a risk are to be:
   a. Specifically pointed to by the risk register
   b. The User Story must point to its relevant risks on the user story.
3. A decision on how to address risk, plus a User Story is to be placed on the backlog to make it actionable.

Summary

It is my belief based on years of managing projects that if one prepares for risk events, then one is much more capable of dealing with them when the time comes. In this chapter, a clear method of dealing with risk and effectively managing it has been shared.

Knowledge Expansion

1. For a project you are working on, use the process indicated above to address three risk events.
2. Create an argument for the handling of one of your risks identified above if the team wants to ignore a risk.