IT Risk Management – Looking Ahead and Fixing the Monsters While They are Small!

by Neil Potter, The Process Group

If you have been involved in any size project, you know that surprises and problems can drain your resources, cause major stoppages or shut down the project all together.

Although not every problem can be foreseen, many can, and any action taken early to avoid, reduce or prepare for problems can be ten times less effort that dealing with the problem later.

In this article I will share a real example of risk management applied to an Enterprise Resource Planning (ERP) project, one that was very successful, in part due to risk management being aggressively applied at the beginning. A summary of the risk process used is described at the end of the article.

The Project

The company in this article manufactures large metal structures used in the oil and gas energy business. Designs are created in the engineering department and submitted to an ERP system for manufacture. The manufacturing area pulls the drawings along with a list of parts needed, and proceeds to manufacture the product.

While manufacturing occurs, the accounting group takes the same information from the ERP system and creates invoices to bill the customer. Other departments use the ERP data to perform product scheduling, resource management, billing, accounting, and supplier tracking activities.

After several years of use, a significant amount of the information in the ERP system was either incorrect, duplicate, or had been moved to spreadsheets stored outside of the system. For example, not all part numbers for manufacturing were correct, invoice and billing codes were used inconsistently. When the system became too difficult and confusing to use, information was stored and shared in local spreadsheets and emails. Additional effort was then needed to reconcile spreadsheet and ERP data so that financial reports could be created.

The job of cleaning up the contents and use of the ERP system was given to the IT group and the CIO. This article describes the risk management activity that was performed when the ERP upgrade project was initially planned.

The Project Team, Project Planning and Cost

Eight senior individuals were selected for the upgrade project from each of the departments that used the ERP system. This covered engineering, project management, manufacturing, accounting, and executive management.
The project team decided to spend four days offsite to scope and plan the upgrade project. Planning involved:

- Scoping the changes to be made
- Estimating the effort required
- Assessing and mitigating risks
- Developing a schedule to complete the work
- Reporting and negotiating cost, schedule and risk options to executive management

The total cost estimate for implementing all changes was $455K over nine months (mostly labor). The project team of eight people would work 60% of their time on the ERP project.

**The Risk Management Process**

During the offsite-planning meeting, one morning was allocated to developing a risk plan. This session was led by the CIO and facilitated by myself.

**Process Overview**

Risk management is an inexpensive and effective method of identifying potential problems (risks), analyzing those risks, planning to manage them, and reviewing them.

**Risk Identification**

Risk identification can be done using a 30-minute brainstorming session. Table 1 lists the initial risks of the ERP project developed during the planning session.

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data loss due to ERP changes.</td>
</tr>
<tr>
<td>2</td>
<td>No clear plan to consolidate accounting books with ERP data.</td>
</tr>
<tr>
<td>3</td>
<td>No infrastructure for ERP user to report problems and communicate back resolutions.</td>
</tr>
<tr>
<td>4</td>
<td>Orders falling between the cracks because ERP usage/knowledge is inadequate (order is missed).</td>
</tr>
<tr>
<td>5</td>
<td>Manufacturing production stops or slows due to ERP issues.</td>
</tr>
<tr>
<td>9</td>
<td>Users do not know how to use new ERP business flows.</td>
</tr>
</tbody>
</table>
Users upset with slow / new ERP system.

ERP upgrade team resources are pulled impacting the ERP deployment schedule.

ERP data changes cause financial regulatory compliance issues (e.g., Sarbanes–Oxley).

Lack of clear ownership of ERP tables and data making modification difficult

Continued lack of process discipline (accuracy, procedural, and timeliness) by users after upgrade.

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Items (Potential Future Problems Derived from Brainstorming)</th>
<th>Consequence</th>
<th>Impact to Project if Risk Item Does Occur (1-10)</th>
<th>Likelihood of Risk Item Occurring (1-10)</th>
<th>Priority (Likelihood x Impact)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>ERP upgrade team resources are pulled impacting the ERP deployment schedule.</td>
<td>Delayed upgrade target dates + ERP users continue to perform workarounds in Excel.</td>
<td>9</td>
<td>10</td>
<td>90</td>
</tr>
<tr>
<td>5</td>
<td>Manufacturing production stops or slows due to ERP issues.</td>
<td>Revenue loss / upset customer</td>
<td>9</td>
<td>10</td>
<td>90</td>
</tr>
</tbody>
</table>

Table 1: Initial risk brainstorm

Risk Analysis

The purpose of analysis is to set priorities and determine where to focus risk mitigation efforts. Some of the identified risks are unlikely to occur and others might not be serious enough to worry about.

During analysis of the ERP risks, each risk item was discussed to understand what might happen if the risk occurred. This brief discussion resulted in a consequence statement being captured as a reminder of the likely result of this risk if no action were taken.

A rating system of 1 through 10 was then used to rank each risk relative to the other ones on the list and generate a final priority. The previous discussion and resulting consequence helped the team derive an impact rating. The ratings and final priority is shown in Table 2.
<table>
<thead>
<tr>
<th></th>
<th>Risk Description</th>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>ERP data changes cause financial regulatory compliance issues (e.g., Sarbanes–Oxley).</td>
<td>Project failure</td>
<td>9 9 81</td>
</tr>
<tr>
<td>13</td>
<td>Lack of clear ownership of ERP tables and data making modification difficult</td>
<td>Data integrity</td>
<td>9 9 81</td>
</tr>
<tr>
<td>14</td>
<td>Continued lack of process discipline (accuracy, procedural, and timeliness) by users after upgrade.</td>
<td>Project fails</td>
<td>10 8 80</td>
</tr>
<tr>
<td>9</td>
<td>Users do not know how to use new ERP business flows.</td>
<td>Many errors entered into ERP</td>
<td>5 7 35</td>
</tr>
<tr>
<td>2</td>
<td>No clear plan to consolidate accounting books with ERP data.</td>
<td>Missed financials / reporting / failing SOX</td>
<td>10 3 30</td>
</tr>
<tr>
<td>4</td>
<td>Orders falling between the cracks because ERP usage/knowledge is inadequate (order is missed).</td>
<td>Revenue loss / upset customer</td>
<td>9 3 27</td>
</tr>
<tr>
<td>10</td>
<td>Users upset with slow / new ERP system.</td>
<td>Reluctant adoption, use 2 systems (old + Excel)</td>
<td>3 8 24</td>
</tr>
<tr>
<td>1</td>
<td>Data loss due to ERP changes.</td>
<td>Financial loss, revenue booking</td>
<td>7 3 21</td>
</tr>
<tr>
<td>3</td>
<td>No infrastructure for ERP user to report problems and communicate back resolutions.</td>
<td>Errors go undetected/resolved</td>
<td>4 2 8</td>
</tr>
<tr>
<td>7</td>
<td>Current ERP system implementation and usage is based on one persons expertise who becomes unavailable</td>
<td>Delays / old orders not closed out</td>
<td>6 1 6</td>
</tr>
</tbody>
</table>

Table 2: Initial risk with priorities

Risk Management Plan
There are two primary actions one can do to manage risk. First, take action to reduce (or partially reduce) the likelihood of the risk occurring. Second, take action to reduce the effect if the risk does occur.
Focus should be placed on reducing the likelihood of the risks occurring since this type of action is typically easier and cheaper early in the project. If the likelihood cannot be reduced enough, and the impact is still high, a backup plan can be generated to allow the team to keep working even if the risk occurs.

In Table 2, the top priority risk is, *ERP upgrade team resources are pulled impacting the ERP deployment schedule*. The total work estimate for the ERP upgrade was nine months and expecting a part-time team of already busy professionals to achieve this was unrealistic. This not only had consequences of the ERP upgrade work not being complete, but promoted growth of the current situation where ERP users would give up on the ERP and use personal spreadsheets.

The following preventative actions were taken to reduce the likelihood of this risk occurring:

- Make two people on the ERP team full-time for at least one year. This meant delegating most of their existing activities to others. To minimize cost, the current activities that were administrative in nature were given to a new administrative assistant.

- Break up the ERP upgrade tasks into small independent chunks and spread them over 9 months with gaps in between allowing the ERP team to move between the ERP work and other work. For example, spend 2 weeks focused on ERP followed by 2 weeks focused on normal work. The next ERP chunk would only be started when the previous one was complete. This also minimized the disruption to the companies work and made it easier to debug problems caused by ERP changes.

- Have each ERP team member identify a back up resource for their normal work should day-to-day issues arise that they cannot attend to.

- Schedule ERP upgrade work to avoid existing company milestones (e.g., quarterly, end-of-month) where ERP team members would be busy with their normal jobs.

- Establish an escalation channel and ERP upgrade management team so that when ERP team members receive requests pulling them off scheduled ERP work, the management team could be fully aware of (and involved in) the decision to delay ERP activities.

As well as preventative actions, the team also considered corrective actions that could be taken if the team members were pulled off the ERP team and assigned to other tasks. These were:

- Change the order of the ERP-upgrade tasks such that the pulled resource is less critical to the current task.

- Delay the ERP schedule.

- Reduce the scope of the ERP upgrade allowing each team member more time for day-to-day duties.

- Escalate the resource issue to the ERP management team for a decision along with recommend options.
The second priority risk was, *Manufacturing production stops or slows due to ERP issues*. Many groups in the company relied on the ERP system to maintain the current production cycle. Products to be built, and the parts needed, were all contained in the ERP database. Any disruption or error in the data because of an ERP change would either stop manufacturing or cause the wrong products to be created.

To avoid this risk the following preventative actions were taken:

- Test each change from order entry to production on a real, but dummy, transaction to ensure that the flow was correct.
- Identify and train all of the stakeholders involved in each ERP change (from order entry staff to shop floor mechanics).
- Generate training materials and checklists that supervisors can use in their own area to train staff as needed.
- Conduct real-time audits to ensure that ERP users are entering data correctly in the ERP system.
- Evaluate the first few uses of each ERP change to capture lessons learned before moving to the next ERP change.

The following backup actions were developed in the event of an ERP change disrupting the order-entry / manufacturing flow:

- Provide hotline support to address the issue real time. Provide a workaround while the issue is addressed.
- Schedule periodic ERP team meetings to determine the underlying cause of the issue (e.g., ERP change, user error, training). Generate corrective actions for chronic ERP issues caused by the change.
- Consider delaying subsequent ERP changes until the current change is operational.
- Notify the ERP management team of the issue so that they can inform their staff.

**Risk Review**

You will want to review your risks periodically so you can check how well mitigation is progressing. You can also see if the risk priorities need to change or if new risks have been discovered. You might decide to rerun the complete risk process if significant changes have occurred on the project. Many people incorporate risk review into other regularly scheduled project reviews.

**What Happened**

The ERP upgrade team did complete its work. The changes were implemented in chunks as planned and training courses, audits and checklists were used to manage each change. The ERP team did get the resources they needed (e.g., eight part-time assistants) and management was involved throughout with no escape from the hard
decisions to either fund the effort or explain to the organization why the ERP system was not improving.

**Summary**

Risk management is a straightforward method to look downstream, assess what could go wrong, and set priorities for what actions to take. It can help a team get its arms around potential chaos, identify small actions that can be taken early with large impact, and cause a mental shift in an organization to deal with potential problems now, rather than hope they will vanish soon.

Risk management actions can cause the right people to get involved early, share ownership of the issues, seek expertise from others and make sure no one is surprised when problems occur.

**Neil Potter**

Neil Potter is co-founder of The Process Group, a company formed in 1990 that consults on process improvement, software engineering, CMMI, Agile/Scrum and project management.

He has 26 years of experience in software and process engineering. Neil is an SEI certified lead appraiser for SCAMPI appraisals, certified high-maturity appraiser, Intro to CMMI instructor (development and services), Six Sigma Greenbelt and Certified Scrum Master.

He has a B.Sc. in Computer Science from the University of Essex (UK) and is the co-author of *Making Process Improvement Work - A Concise Action Guide for Software Managers and Practitioners*, Addison-Wesley (2002), and *Making Process Improvement Work for Service Organizations*, Addison-Wesley (2012).

He can be reached at:

Cell/text: 972 418 9541
neil@processgroup.com
http://www.processgroup.com
Risk Management Process

1. Determine scope of the risk session.

2. Select the team and moderator.

3. Identify risks (potential future problems)
   - Brainstorm areas of risk, e.g., weak areas such as unknown technology, tools, target machine
   - Things that are critical or extremely important to the effort, such as the timely delivery of a vendor’s database, creation of translators, or a user interface that meets the customer’s needs
   - Things that have caused problems in the past, such as loss of key staff, missed deadlines, or error-prone software.

Remove invalid or irrelevant items. Current problems should be treated as problems, not risks.

4. Analyze risks.

   For each risk item:
   - Does the team understand the risk item? If necessary, split into separate risk items, e.g.,
     - “People may leave the project” could be restated as, “Accountant might leave the project,” and “ERP expert might leave the project.”
   - Discuss and determine its scope; What would the consequences be if this risk item did happen?
   - Determine what the impact would be if the worst happened, using a scale of 1-10.
   - Determine how likely it is that the risk item will occur, using a scale of 1-10.
   - Determine the priority of the risk items and thus which to work on (impact x likelihood).

5. Plan to mitigate risks.

   - Select the most important risk issues, such as the top two or three, or top 20%.
   - Brainstorming on actions that could be taken to reduce the likelihood of the risk item occurring.
   - Decide which actions to pursue.
   - Select a person to be responsible for each action chosen.
   - Document the information in the risk management plan.


   - Establish how often risks should be reviewed (once a month is typical). Risk reviews can be incorporated into existing project status and phase reviews.
• Update the list based on risk review sessions.