Risk Management: Pro-active Principles for Project Success

Liz Markewicz
Don Restiano
What is a Risk

According to the Defense Acquisition University:

“Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule and technical constraints”

ISO Defines Risk as the:

- “combination of the probability of an event and its consequence”
What is a Risk

In other words:

- Risk is anything that *could* cause a negative cost, schedule, or performance impact
  - Must have a probability of *less than 100%*; anything with a probability of 100% isn’t a risk, it’s an issue or a problem.

Identifying Risks provides an opportunity to avoid negative impacts
Risk Vocabulary

- Risks
- Problems
- Worries
Risk Vocabulary

Risk is …the **Possibility Of Suffering A Loss**, the uncertainty of attaining a future goal – *it hasn’t happened yet*.

Every Risk has Two Elements

- **Probability**: the chance that an event will occur. If it’s a sure thing, then it’s a problem (not a risk)
- **Consequence**: A negative impact on Cost, Schedule, Performance or a combination of all three…”then”

**Probability**: The likelihood that an event will occur ( <100% ).

**Undesirable Consequence**: The negative impact if the risk occurs: Cost will increase, Schedule will be delayed or Performance will be degraded.
What RISK is NOT…

- **Problem** is a negative consequence with a certain, or almost certain probability of occurrence. It is not a risk
  - Problems need to be dealt with via corrective action but not as part of Risk Management.
    - They can **not** be Mitigated or Avoided

- **Worries** are small scale, routine, day-to-day uncertainties that your normal processes should account for (e.g.; equipment calibration and maintenance cycles or System upgrades)
  - Worries are **Not** considered risks
  - ‘Standard operating procedure’ usually handles

Risks can be avoided – Problems can’t
What is Risk Management?

- A proactive, customer-focused approach to manage uncertainty
- Risk Management is a continuous, closed loop process that captures new risks as they emerge, tracks the status of already identified risks, retires risks through successful actions, or realizes risks through unsuccessful actions

Risk Management is a systematic process to ID, assess & manage risks
Why Use Risk Management?

Companies can’t afford to fail

• “S*#! happens”: Projects often fail because of unexpected or unmitigated risks….the ‘known unknown’
  ◆ The results of an Aberdeen Group study showed that manufacturers without best-in-class risk management procedures were twice as likely to suffer a major impact. Industry Week, Blanchard, Feb 2009

• Failure to manage risks usually leads to:
  ◆ Budget Impacts - increased cost,
  ◆ Schedule Impacts - delays,
  ◆ Performance Impacts - defects
  ◆ Career & Business Impacts - unhappy management and customers.

• Risk Management contributes to project success
  ◆ Proactive not Reactive - An ounce of prevention is worth a pound of cure
    – ID what could happen & you can try to avoid rather than ‘brace for impact’
    – No one is blindsided

Properly managed, risks can be controlled
Why Use Risk Management?

Successful businesses spend $ on activities that produce results.

- Risk Management helps optimize resource utilization
  - Identifies what could go wrong
  - Assesses Probability & negative Consequence of it occurring
  - Develops potential mitigation, its cost, and potential to reduce the risk
  - Allows comparison:
    - Mitigation vs. Wait and See
    - Allocating resources to one risk vs. another

- Successful Mitigation plans minimize cost, schedule & performance problems

Risk Management supports knowledge-based decision making
The Risk Management Process

- We’ll go thru the basic approach & concepts and then follow this up with a case study concerning reliability and the application of risk management
The Risk Management Process

- 5 steps - derived from a process developed by the Defense Acquisition University, and other sources such as Carnegie Mellon’s Software Engineering Institute and the Open Systems Initiative.

- Process Steps
  1. Plan
  2. Identify Risks
  3. Assess and Prioritize Risks
  4. Develop and Implement Risk Handling Approaches
  5. Track and Report

Risk Management is an ongoing process, not an event.
Step 1 – The Risk Management Plan

The ‘blueprint’

- Defines the structured, disciplined process: the who, what, how and when that is required to identify and manage risk
  - Responsibilities and Stakeholders
  - Oversight and Reporting requirements
  - Selected Tools
  - Parameters for risk categorization
  - Thresholds that trigger mitigation activity

- Standardized scales for Probability & Consequence assessment
  - May tailor for Projects
  - Consistently apply across entire project for the duration

- Does **not** identify the risks

Plan Provides the Framework. NOT the risks
Step 2: Risk Identification

What are all the risks to the project or program

- Techniques for Risk ID can include:
  - Brainstorming
  - Expert interviews, Lessons Learned
  - Failure Modes and Effects Analyses (FMEAs)
  - Staffing Evaluations
  - Review Requirements
    - Are there any TBDs?
    - Are any requirements inadequately defined?
    - Are any requirements very difficult to meet?
- Filter out the Problems and the Noise
- Assign a Risk Owner
  - Ownership is based on who can most likely effect a positive outcome, not by who is most affected by the consequences

Make Risk ID an ongoing practice, not an event
Step 2: Risk Identification

Develop a Risk Statement for each

• A Good Statement…
  • Is concise and quantitative
  • Captures the consequence in the statement
  • Uses an if…then format
    – IF (conditional probability)
    – THEN (consequence)
Step 3 - Risk Assessment and Prioritization

Assess each risk:
What’s the Probability ($P_f$) & Consequence ($C_f$) of each?

- Standardize Measure of Probability ($P_f$) & Consequence ($C_f$):
  - Should be defined in the Risk Management Plan
  - Specific Categories for Pf and Cf
  - Ensures Risks are normalized (a high risk is a high risk is a high risk)

- $P_f$ and Cf can be Qualitative (Hi/Med/Low) or Quantitative
  - Quantifying Consequence is preferable
    - Puts ceiling on mitigation spending
    - Generates more proactive response to risk
Step 3 - Risk Assessment and Prioritization

Prioritize: Which pose the greatest threat to the project?

- The Risk Factor ($R_f$) is an evaluation of a Risk’s probability of occurring and the severity of consequence to determine its overall seriousness

\[(P_f \times C_f) = R_f\]

- Prioritizing = Ranking all risks by Risk Factor

- Get consensus of assessment from all stakeholders
  - Apply reality check

- Reassess periodically or when conditions change
  - Are your actions producing the expected results?
Step 4 - Risk Handling

Five Approaches

- **Avoidance**: Adopt a baseline that doesn’t allow the risk to occur.
  - Ex: Changing requirements while still meeting end product needs.

- **Transfer**: Require a 3rd party, (supplier, subcontractor, etc) to share the consequence if the risk is realized.
  - Ex: Reallocating requirements to a party that has more control over the risk area
  - May be implemented via contract penalties/incentives, insurance policies, etc

- **Assumption**: Risk is acknowledged and accepted, but no actions are taken.
  - E.g.; Cost to mitigate > impact value; have no control over the risk, strategy for a low risk.
  - Resources may be set aside in reserve to absorb the impact of the risk should it occur

- **Contingency Planning**: Identify activities to invoke if the risk is realized. ID Contingencies when there’s insufficient confidence in the mitigation activities, or when there are no viable activities that could reduce or control a risk

- **Mitigation**: Define & Implement actions to control/minimize risk.
  - The most proactive means of handling risks
Step 4 - Risk Handling

Elements of a good mitigation plan:

- **Action oriented**
  - Mitigation steps address the root cause & reduce the \( R_f \)
  - “Monitor’ is **not** Mitigation

- **Cost Benefit from mitigation > cost to mitigate**

- **Has Start and End dates for each step**

- **Ownership & Resources**

- **Success criteria (How much is ‘enough’)**
  - Defines the expected outcome for **successful** completion of the step
  - Not always required to mitigate risk probability to zero

*Preventive not Corrective*
Step 5 – Track and Report

- Risks and mitigation should be tracked & reported regularly
  - Make it a habit not an event
  - Enforce Accountability and Visibility
    - Regular reviews of risks with key stakeholders
    - Risks periodically reviewed by management

- How are planned actions proceeding
  - Was the Risk Mitigated?
  - Has the Risk Increased?
    - Time to re-evaluate the plan of attack?
  - Any new risks?
Case Study:

The XYZ Communications Module Upgrade
The XYZ company designs and manufactures a communication system consisting of a power supply, transmit and receive module, and a controller card. They typically build and then perform a formal acceptance test for their customer, which they have to pass in order to be able to sell off the lot. They update the design due to tech refreshes and obsolescence every few years.

The design/build/test cycle was 18 months for the original design. The next two iterations had minor capability upgrades. The first took 15 months, the second 12 months.
Because XYZ had been consistently cutting down their cycle time, they agreed to a 12 month schedule for the newest iteration of the design, same as the last build. But there were some differences this time around.

- New transistor technology in the transmit/receive circuitry to handle higher power requirements
- Power Supply will stay the same, but will now be stressed at a higher level due to the increased power requirements
- New vendor for the controller card, who claims that the controller firmware will interface with the Power Supply and Transmit/Receive Module, but this has not been tested
Case Study (continued)

- Although warning signs were present that this was an aggressive schedule, no risks were formally identified and no plan was put in place to handle them. As it turned out:
  - The new transistor technology was unable to meet specifications without extensive additional testing and modifications from the supplier
  - The power supply handled the increased power load, but the extra heat it dissipated resulted in changes in the mechanical layout of the system
  - The new Controller Card firmware had to be modified to work with the existing power supply and transmit/receive module
- All of these factors caused XYZ to enter the acceptance test over budget, behind schedule, and with a reduced degree of confidence they would pass the test
- What could XYZ have done differently? And how could a robust Risk Management Program have helped them to avoid these problems?
Step 2: Risk Identification

- **Example from Case Study:** New vendor for the controller card claims that the controller firmware will interface with the Power Supply and Transmit/Receive Module, but this has not been tested.

- **Example of a good risk statement:** IF the firmware in the new controller card is unable to communicate with the Transmit/Receive Module and Power Supply, THEN modifications to the firmware or selecting new hardware will be required, causing an increase in budget and jeopardizing the current schedule.
Step 3 - Risk Assessment and Prioritization

Example from case study: Perform a quantitative assessment of the risk that the firmware in the new controller card will communicate with the Transmit/Receive Module and Power Supply.
### Step 3 - Risk Assessment and Prioritization

<table>
<thead>
<tr>
<th>Rating</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>Theoretical S/W concepts beyond known practice. Development of new approach &amp;/or language.</td>
</tr>
<tr>
<td>0.8</td>
<td>New complex S/W, new approach, new language. New unproven apps. Extremely large scale integration.</td>
</tr>
<tr>
<td>0.7</td>
<td>All new S/W development, beyond experience base. Large integration of new or existing S/W.</td>
</tr>
<tr>
<td>0.6</td>
<td>Extensive changes in S/W development approach &amp; application. Moderate integration of new or existing S/W.</td>
</tr>
<tr>
<td>0.5</td>
<td>Major modification of approach, conversion from similar S/W, expanded to new application. Some Int Exp</td>
</tr>
<tr>
<td>0.4</td>
<td>Moderate modification &amp; tailoring of existing S/W but team was design agent with integration experience.</td>
</tr>
<tr>
<td>0.3</td>
<td>Slightly modified S/W &amp;/or combining of existing functions with minor integration. Team was design &amp; Int. agent.</td>
</tr>
<tr>
<td>0.2</td>
<td>Some modification of existing S/W approach with minimal integration impacts. Team was design &amp; Int. agent.</td>
</tr>
<tr>
<td>0.1</td>
<td>Minor revision and checkout of existing software. No impacts to integration tests.</td>
</tr>
<tr>
<td>1.0</td>
<td>Use of existing, checked out S/W. No additional test, validation or integration required.</td>
</tr>
</tbody>
</table>

### Probability of Occurrence (P_f)

<table>
<thead>
<tr>
<th>Software</th>
<th>Testing</th>
<th>Technology</th>
<th>Hardware</th>
<th>Producibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
<td>Theoretical technology, design or concepts beyond known testing processes, methods or practices.</td>
<td>Maximum theoretical technology; max or beyond known capability</td>
<td>Theoretical design capability; max or beyond known research. Real or potential R&amp;D breakthrough.</td>
<td>0.9</td>
</tr>
<tr>
<td>0.8</td>
<td>Theoretical technology, design or concepts requiring significant research in testing methods, processes or practices.</td>
<td>Theoretical Technology requiring significant research.</td>
<td>New Theoretical concepts beyond known capability or technology to support new concepts or significant R&amp;D exploration and development.</td>
<td>0.8</td>
</tr>
<tr>
<td>0.7</td>
<td>Technology approach has identified conceptual test methods but not verified or validated.</td>
<td>Newer technology; feasible by analogy; Concept untested or not verified.</td>
<td>All new complex S/W, design &amp; Int. approaches require testing of many new HW elements.</td>
<td>0.7</td>
</tr>
<tr>
<td>0.6</td>
<td>Technology approach has limited conceptual testing. Limited or no in house experience.</td>
<td>Newer technology; feasible by analogy, studies and/or concept verification.</td>
<td>New design to moderately improved existing design &amp;/or major integration of many HW elements.</td>
<td>0.6</td>
</tr>
<tr>
<td>0.5</td>
<td>New technology or similar designs have initial testing. Limited or no in house experience</td>
<td>New &amp;/or adapted technology with feasibility studies and initial testing.</td>
<td>Major design modifications &amp;/or major integration of many HW elements.</td>
<td>0.5</td>
</tr>
<tr>
<td>0.4</td>
<td>Similar designs &amp; technology have been tested by other design agencies. Limited in house experience.</td>
<td>Proven technology and approach.</td>
<td>Redesign, rework or extensive mod of existing integrated design.</td>
<td>0.4</td>
</tr>
<tr>
<td>0.3</td>
<td>Limited testing done on new or existing components but experienced in test methods.</td>
<td>Proven technology and approach; previously validated.</td>
<td>Existing proven components, recombined or minor modifications.</td>
<td>0.3</td>
</tr>
<tr>
<td>0.2</td>
<td>Sub systems &amp;/or components are tested for current application or validated in similar applications.</td>
<td>Proven technology and approach. Used occasionally by a design agent</td>
<td>Existing proven components, recombined or minor modifications &amp;/or minor usage variation.</td>
<td>0.2</td>
</tr>
<tr>
<td>0.1</td>
<td>System has been tested &amp; validated in similar applications.</td>
<td>Proven technology and approach with significant design experience.</td>
<td>Functional HW. Mods in form only. Minor usage variation.</td>
<td>0.1</td>
</tr>
<tr>
<td>1.0</td>
<td>System has been thoroughly tested &amp; validated for current application.</td>
<td>Off-the-shelf hardware proven to operational environments</td>
<td>Functional hardware. Hardware will meet the form, fit, &amp; functional reqmts. of the application</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**P_f (Software) = 0.4** (Moderate modification of existing S/W)

**P_f (Testing) = 0.3** (Limited testing done on new or existing components but experienced in test methods)
### Step 3 - Risk Assessment and Prioritization

#### Potential Severity of Consequences ($C_f$)

<table>
<thead>
<tr>
<th>Rating</th>
<th>Program Threat</th>
<th>Cost Impact</th>
<th>Schedule Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Program threat is certain</td>
<td>Major prog. Milestones moved; Prog &gt; 9 months threatened</td>
<td>Program Slip</td>
</tr>
<tr>
<td>0.9</td>
<td>Major program contract</td>
<td>Changes require revision w/cust.</td>
<td>NRE &gt; 70K$ or 17.5% Unit &gt; 7K$ or 17.5%</td>
</tr>
<tr>
<td>0.8</td>
<td>Affected cost goal in jeopardy.</td>
<td>Significant rebudgeting reqd.</td>
<td>NRE &gt; 60K$ or 15% Unit &gt; 6K$ or 15%</td>
</tr>
<tr>
<td>0.7</td>
<td>Changes require revision w/cust.</td>
<td>Some rebudgeting required.</td>
<td>NRE &gt; 50K$ or 12.5% Unit &gt; 5K$ or 12.5%</td>
</tr>
<tr>
<td>0.6</td>
<td>Significant rebudgeting reqd.</td>
<td>Some program changes; critical path affected.</td>
<td>NRE &gt; 40K$ or 10% Unit &gt; 4K$ or 10%</td>
</tr>
<tr>
<td>0.5</td>
<td>Some rebudgeting required.</td>
<td>Subsystem slip within IPT Requires workaround.</td>
<td>NRE &gt; 30K$ or 7.5% Unit &gt; 3K$ or 7.5%</td>
</tr>
<tr>
<td>0.4</td>
<td>Changes within mgmt reserve.</td>
<td>Subsystem slip within IPT Requires workaround.</td>
<td>NRE &gt; 20K$ or 5% Unit &gt; 2K$ or 5%</td>
</tr>
<tr>
<td>0.3</td>
<td>Minor within budgeted range</td>
<td>Minor changes to internal IPT milestones</td>
<td>NRE &gt; 10K$ or 2.5% Unit &gt; 1K$ or 2.5%</td>
</tr>
<tr>
<td>0.2</td>
<td>Budget reallocated within current plan.</td>
<td>Possible minor slip, noncritical path.</td>
<td>NRE &gt; 10K$ or 2.5% Unit &gt; 1K$ or 2.5%</td>
</tr>
<tr>
<td>0.1</td>
<td>Negligible cost increase</td>
<td>Possible minor slip, noncritical path.</td>
<td>NRE &gt; 10K$ or 2.5% Unit &gt; 1K$ or 2.5%</td>
</tr>
</tbody>
</table>

* Values are for example only. Scale to fit individual program or project budget and schedule.

NRE: Non-recurring Expense

---

- **Cf (Cost) = 0.5** (Some rebudgeting required, estimate NRE cost at $50K)
- **Cf (Schedule) = 0.2** (Estimate 1 ½ month schedule impact)
Step 3 - Risk Assessment and Prioritization

– Example from case study: Perform a quantitative assessment of the risk that the firmware in the new controller card will communicate with the Transmit/Receive Module and Power Supply.

  – $P_f = 0.4$ (Highest of assessed $P_f$ factors)
    » $P_f$ (Software) = 0.4 (Moderate modification of existing SW)
    » $P_f$ (Testing) = 0.3 (Limited testing done on new or existing components but experienced in test methods)

  – $C_f = 0.5$ (Highest of assessed $C_f$ factors)
    » $C_f$ (Cost) = 0.5 (Some re-budgeting required, estimate NRE cost at $50K)
    » $C_f$ (Schedule) = 0.2 (Estimate 1 ½ month schedule impact)

  – $R_f = P_f \times C_f = 0.4 \times 0.5 = 0.2$

– Get consensus of assessment from all stakeholders
– Document all rationale and assumptions
### Step 4 - Risk Handling

- **Example from case study:** Options on handling the risk that the firmware in the new controller card will communicate with the Transmit/Receive Module and Power Supply.

<table>
<thead>
<tr>
<th>Avoidance</th>
<th>Assumption</th>
<th>Transfer</th>
<th>Mitigation</th>
</tr>
</thead>
</table>

- **Transfer Risk to Supplier**
  - Supplier claims that modifications to firmware will be minimal and that they will not impact overall schedule
  - Get supplier to agree to a firm fixed price contract to perform the work, not based on hours required
  - Provide a fee structure based on delivery date, incentive for early delivery, penalty for late delivery
Step 4 - Risk Handling - Mitigate

- Example from case study: Use the option to “Mitigate” the risk that the increased power requirements for the Power Supply will cause a thermal issue for adjacent components.
- Mitigate by performing a thermal and stress analysis under the new load conditions prior to laying out the new module design.
- Elements of a good mitigation plan
  - Risk Reduction
    » Make sure each step (or group of related steps) reduces your \( P_f \) or \( C_f \). Otherwise, why perform that step?
  - Cost Benefit
    » The cost of performing the step must be worth the benefit gained by completing the step.
  - Schedule Benefit
    » Clearly identify the start and complete dates of each step.
    » Make sure they support the overall schedule.
  - Clearly define success
    » What are the expected results of the analysis that will show the step successfully lowers the risk.
## Step 4 - Risk Handling - Mitigate

<table>
<thead>
<tr>
<th>STEP #</th>
<th>START</th>
<th>COMPL</th>
<th>DESCRIPTION</th>
<th>RESP. ENG.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DATE</td>
<td>2/1/2010</td>
<td>3/1/2010</td>
<td>Joe Stress</td>
</tr>
<tr>
<td></td>
<td>PF</td>
<td>0.5</td>
<td>0.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CF</td>
<td>0.6</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RF</td>
<td>0.3</td>
<td>0.24</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>DATE</td>
<td>3/1/2010</td>
<td>5/1/2010</td>
<td>Joe Thermal</td>
</tr>
<tr>
<td></td>
<td>PF</td>
<td>0.4</td>
<td>0.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CF</td>
<td>0.6</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RF</td>
<td>0.24</td>
<td>0.12</td>
<td></td>
</tr>
</tbody>
</table>

**Step 1 Stress Analysis**

Perform electrical stress analysis to verify that no components are stressed beyond their derating guidelines. Reduces Pf from 0.5 to 0.4.

**Step 2 Thermal Analysis**

Perform thermal analysis to verify that case temperature of the power supply does not exceed 60 degrees C., so that module component re-layout will not be required. Reduces Pf from 0.4 to 0.2.
Summary

- A Risk Has To Have Two Components
  - Probability Of Occurrence Less Than 100%
  - Negative Consequence (Cost, Schedule, Performance, Etc.)

- Risk Management vs. Crisis Management
  - Proactive vs. Reactive
  - Pay Me A Little Now Or A Lot Later

- Risk Management is a closed loop process
  - Plan, Identify, Assess, Handle, Track and Report

- Multiple Options To Handle Risk
  - Avoidance, Assumption, Transfer, Mitigation

- Be Part Of The Solution, Not Part Of The Problem
  - Identifying risks is everyone’s responsibility
  - Don’t be the “I knew that was going to be a problem” person after the risk becomes a problem!
Why Risk Management?

“If Risk Managers help prevent potential problems from occurring; Then…”

Risk Management = Genius!
Questions?