Quantify Risk Tolerance to Guide Risk Policy

ERM009

Speakers:
Joseph W. Mayo, President, J.W. Mayo Consulting, LLC
Jeff Vernor, Sr. Director, ERM and Internal Audit, TPG Global, LLC
Learning Objectives

At the end of this session, you will:

• Understand how to use tolerance and appetite to shape ERM policy
• Learn tools and techniques that can be used to objectively quantify risk impact
• Understand the relationships between risk policy, tolerance, appetite, and reserve budgets
• Understand the impact of ineffective Enterprise Risk Management by reviewing two real-world case studies
Agenda

• Introduction
• Risk policy, risk appetite, risk tolerance, and reserve budgets
• Objectively quantify risk appetite and tolerance
• Tools and Techniques
• Case Studies
  – Deepwater Horizon
  – US Government
• High Reliability Organizations (HRO)
• Conclusion
• Q&A
Introduction

• Joseph Mayo, PMP, RMP, CRISC
• 30 years in the IT industry primarily focused on risk and project management
• Career highlights include:
  – Program Manager for Project #7 of InfoWorld's Top 100 IT Projects of 2006
  – Developed a risk management maturity roadmap for a U.S. Government Agency
  – Instrumental in the development and approval of Government Agency risk policy
  – Developed an IV&V Program that was recognized by the Government Accounting Office (GAO) as a model for large complex Government programs
  – Author of Chaos to Clarity – The Tao of Risk Management

• joseph.mayo@jwmc-llc.com
Introduction

• Jeff Vernor, MBA, CCSA, ARM
• 20 years in the risk management field with the last 16 in financial services ERM
• Career highlights include:
  – Chair of RIMS ERM Committee; contributing author to several RIMS publications
  – Guest lecturer at ten different universities with specialties in ERM and insurance
  – Helped build ERM from scratch at two leading financial services firms
  – Expertise on operational risk, enterprise risk, insurance, and safety
  – Prior to TPG, served as Director of Global Operational Risk at Russell Investments in Seattle and Executive Director, ERM at USAA in San Antonio

• jvernor@tpg.com
1. Who has an established risk appetite?
   - If yes what was the hardest part?
   - What was the key to success?
2. For those who have tried and failed, where do you think it went wrong?
3. What do you believe is the most valuable aspect of establishing a formalized risk appetite?
Policy, Appetite, and Tolerance

- **Risk Policy or Risk Principles** – a statement describing the types of risk and the amount of risk exposure an organization is willing to entertain
  - Policy statement
  - Risk appetite
  - Risk tolerance
  - Roles and responsibilities
  - Governance

- **Risk Appetite** – Desire or craving for taking risk
  - Risk appetite is conceptually similar to human appetite
  - Risk appetite cannot exceed the organization’s risk capacity
  - Six risk contexts; Budget, Schedule, Quality, Mission, Reputation, and Safety

- **Risk Tolerance** – degree of variance from a stated appetite or threshold
Policy, Appetite, Tolerance, and Budgets

• Risk appetite, risk tolerance, and reserve budgets guide the development of risk policy or risk principles
  – These can and should change over time as market conditions change
• Appetite and tolerance drive all aspects of risk management including Governance, treatment strategies, prioritization, reserve budgets, and risk management processes
  – These are strategic risk management elements
• Mandating that project teams manage risk is insufficient and does not constitute ERM
• Effective risk management requires a risk policy or principles that clearly establishes appetite, tolerance, and waiver-ability
Risk Appetite and Tolerance

- Risk policy or principles must explicitly state appetite
  - Enterprise appetite
  - Project appetite
  - Regional/business line differences

- Risk policy or principles must state whether the organization allows waivers
  - If waivers are allowed, risk policy must define or reference pre-defined waiver and governance processes
  - Waivers and tolerance go hand-in-hand

- If possible, objectively quantify appetite and tolerance
  - Based on organizational goals and objectives

- Risk impact must be properly valued and may include impact bands
### Risk Appetite and Tolerance

- **Excerpt from the University of Edinburgh Risk Policy**

The University's appetite for risk across its activities is provided in the following statements, and is illustrated diagrammatically.

<table>
<thead>
<tr>
<th></th>
<th>Unacceptable to take risks</th>
<th>Higher Willingness to take risks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Reputation</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Compliance</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Financial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education &amp; Student Experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Development</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major change activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment and Social Responsibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>People and culture</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Appetite and Tolerance

*Financial* – The University aims to maintain its long term financial viability and its overall financial strength. Whilst targets for financial achievement will be higher, the University will aim to manage its financial risk by not breaching the following minimum criteria:

It will

- achieve a surplus of a minimum of 2% of gross income over any 3 year period
- operate with a Staff Cost/Total Expenses ratio of less than 60%
- achieve a rate of return of at least 2% above inflation on its endowment investments over a 3 year period
- ensure long term borrowings never exceed 20% of net assets
- ensure its surplus before interest always exceeds 2 times net interest charge
- ensure that at least three months equivalent spend is held cash or cash equivalents or in negotiated bank facilities

Why Quantify Objectively?

• A poll of random people revealed interesting answers to the following questions
  -- What is a high budget amount?
  -- What is a long duration?

<table>
<thead>
<tr>
<th>High Budget</th>
<th>Long Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 Trillion</td>
<td>50 years</td>
</tr>
<tr>
<td>$50 Billion</td>
<td>5 years</td>
</tr>
<tr>
<td>$20 Million</td>
<td>10 years</td>
</tr>
<tr>
<td>$3.5 Million</td>
<td>5 years</td>
</tr>
</tbody>
</table>
Why Quantify Objectively?

• Large government agency normalizes risks using a concept called a Risk Adjusted Cost (RAC)
  – $225,000 impact and “High” probability yields the same RAC as $175,000 impact and “Very High” probability
  – The RACs are equal however, there is more than 20% difference in the impact
  – In this case the RAC causes equal treatment when in fact, the $175,000 risk should have a higher priority because of the higher probability of occurrence

• NASA normalized foam strikes as a simple “maintenance” issue, and not a concern for mission success of Space Shuttle Columbia¹
  – Foam from the fuel tank had struck the wing on at least 12 previous shuttle flights, each time causing gouges or other damage
  – Acquiescence to recurring risks has been termed “normalized deviance”

Why Quantify Objectively?

• Helps avoid personal perceptions influencing risk management actions
• Helps avoid normalized deviance
• Simplifies metrics collection and reporting
Risk Budgets

- Management reserve used to manage opportunities and Black Swan events
- Contingency reserve used for all risk management activities
- Project budget of for executing planned activities
- Reserve budgets are separate from project budgets
- Risk governance is the mechanism for transferring risk budget to project budget through RRB
Tools for Quantifying Appetite & Tolerance

• Leveraging ISACA’s Risk IT, Risk Appetite Risk Map
• Expected Monetary Value (EMV) Charts (aka Decision Tree)
Risk IT Risk Map

Risk IT is an excellent guide to understand what constitutes acceptable vs unacceptable risks.

ISACA’s RiskIT is an excellent guide
- Understand what constitutes acceptable vs unacceptable risks
- Understand how much stakeholders are willing to spend for risk treatment
- Objectively quantify appetite
- Properly value risk impact
- Understand risk tolerance thresholds

Risk IT Risk Map

<table>
<thead>
<tr>
<th>Risk Context</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budget</td>
<td>Dollars</td>
</tr>
<tr>
<td>Schedule</td>
<td>Day, Weeks, Months</td>
</tr>
<tr>
<td>Quality</td>
<td>Defects, Rework Dollars/hours</td>
</tr>
<tr>
<td>Mission</td>
<td>Operational Impact (e.g. # Enterprise goals not met)</td>
</tr>
<tr>
<td>Reputation</td>
<td>Customer Satisfaction Survey results</td>
</tr>
<tr>
<td>Safety</td>
<td>Accident impact (e.g. loss of life, lost work days)</td>
</tr>
</tbody>
</table>
- 26 risks represent a total risk exposure of $72M
- Highlighted risks represent 15% of the identified risks and 38% of total exposure
EMV Scenario

- Choose most cost effective travel from Boston to Chicago
- Risk statement: IF travel cost exceeds $350 THEN cancel trip

- EMV Charts are constructed left to right
- ■ - Decision node
- ● - Chance node
- The sum of all chance nodes on a branch must equal 100%
- EMV values are computed right to left
Airplane, Train, or Automobile?

- **Airplane**
  - Direct or Connection?
    - Direct (Invest $349)
      - EMV ($146.50)
    - Connecting (Invest $466)
      - EMV ($496)
      - On-time Arrival
        - Sales $225
          - ($349)
      - On-time Arrival
        - ($466)

- **Train**
  - Direct or Connection?
    - Direct (Invest $391)
      - ($391)
    - Connecting (Invest $631)
      - ($631)

- **Automobile**
  - Non-stop or overnight stay?
    - Overnight Stay (Invest $343)
      - ($343)
    - Non-stop (Invest $194)
      - ($194)
Case Studies
Deepwater Horizon

- Deepest oil well in history at more than 35,000 feet
- Spill cleanup procedures and technology in 2009 were essentially unchanged since the 1960s
- Prior to the Deepwater Horizon disaster, BP considered deep water blowouts in the Gulf of Mexico a high-level risk


Deepwater Horizon

• BP’s Oil Spill Response Plan presented worst case spill scenarios ranging from 28,033 to 250,000 barrels (Davis, 2012)
• Between 1937 and 2010 there were at least 59 oil spills ranging from 29,000 barrels to 6 million barrels.
• BP’s spill scenarios undervalued spill risk by more than 2,400%
  – Average spill size of 59 spills was 741,000 barrels
  – Top 10 of 59 spills ranged from 1 - 6 million barrels and averaged 2.3 million barrels
• U.S. DOI exempted BP's drilling operation from a detailed environmental impact analysis
  – Three reviews of the area concluded a massive oil spill was unlikely (Eilperin, 2010)
• U.S. Minerals Management Service (MMS) approved the spill response plan

Government Agency

- 2,229 software defects identified through tool-based code analysis
- 142.7 hours * 2,229 defects = 318,078 hours of effort to correct all of the unreported defect
  - 142.7 - Average effort over hundreds of defect remediation efforts spanning more than 2 years
- Multiplying $95 per hour times 318,078 yields a total risk exposure of $30.2 million
- Customer could not accept the fact that there was $30M risk exposure
- Boehm and Basili’s research shows a defect that gets deployed costs $14,102 to correct
- Multiplying the 2,229 defects by $14,102 equals $31,433,358
High reliability Organizations (HRO)

- Operate in environments where potential for disaster is high
- Very high risk tolerance
- Top priority is effective performance
- Avoid disasters through collective learning
- Develop a culture of reliability
- Even firms without such catastrophic outcomes from risk events can leverage the models used by HROs

High reliability Organizations (HRO)

• **Five characteristics of a high reliability organization (HRO)**
  1. extensive process auditing procedures
  2. reward system that rewards risk mitigating behavior
  3. quality standards that exceed referent industry standards
  4. correctly assess risks and their associated impact
  5. strong command and control structure consisting of
     • migrating decision making
     • redundancy
     • rules and procedures
     • Training
     • situational awareness

## Compare and Contrast HRO w/ Case Studies

<table>
<thead>
<tr>
<th></th>
<th>Deepwater Horizon</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extensive process auditing procedures awareness</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Reward system that rewards risk mitigating behavior</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Quality standards exceed referent industry standards</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td><strong>Tactical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correctly assess risks and their associated impact</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Migrating decision making</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Redundancy</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Rules and procedures</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Training</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Situational</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

● - Fully implemented  ● - Partially implemented  ○ - Not implemented
Conclusion

• Simplicity is the key to success
• Quantifying risk elements does not require sophisticated tools
  – Effective process and disciplined execution are critical success factors
• If possible, quantitative appetite, tolerance, and impact help avoid normalized deviance (lean toward science and away from art)
  – Imitate HROs (e.g. effective performance, collective learning, culture of reliability)
• Proper risk valuation can avoid catastrophic risk impacts
  – Imitate HROs (e.g. reward risk mitigating behavior, correctly assess risks and their associated impact)
• Effective ERM requires strategic and tactical elements that are complementary
Q&A

- Joseph Mayo
  - www.jwmc-llc.com
  - joseph.mayo@jwmc-llcc.com
  - @TaoOfRisk
  - 571-314-6661

- Jeff Vernor
  - jvernor@tpg.com
  - 817-871-4822