Implementing Enterprise Risk Management in State Government

Drew Zavatsky
Risk Management Division
Office of Financial Management
A recent paper by four Federal Reserve economists, “Making Sense of the Subprime Crisis,” analyzed possible causes of the financial crisis. They surveyed the published research reports by Wall Street analysts and economists, and asked why the Wall Street experts failed to foresee the surge in subprime foreclosures in 2007 and 2008. The Fed economists concluded that the risk models used by Wall Street analysts correctly predicted that a drop in real estate prices of 10 or 20 percent would imperil the market for subprime mortgage-backed securities. But the analysts themselves assigned a very low probability to that happening.

Lessons Learned in Washington

- ERM in Washington State Government
- Review of ERM Agency Training Session
- Reflection on Implementing ERM
- Q & A
ERM Works in Washington

- In 2006, Governor Gregoire named ERM as a ‘best practice’ for all 165 state agencies

- OFM Risk Management Division charged with helping all agencies implement robust ERM programs

- Agencies held accountable for their ERM implementation efforts

- ERM progress is reported every quarter to the Governor in her Government Management, Accountability and Performance (GMAP) forums

- Washington is meeting the challenge!
Why It Works

- ERM is flexible
- ERM is inexpensive to implement
- ERM is easy to learn and use
- We believe that any organization can obtain value through implementing ERM
- In Washington, ERM fits with the management theories and practices already used by every agency
Where We Started From . . .

- Our goal:
  Foster ERM implementation in all 165 state agencies

- Our risks:
  - No Sovereign Immunity
  - Resource Challenges
  - Management Framework
  - Logic Model
Governor’s Management Framework

**PLAN**
- Strategic Plan guidelines
- Logic model
- Baldrige assessment tool
- Customer & constituent feedback

**ALLOCATE**
- Budget Instructions
- Budget Development System
- Agency allotment process
- POG team guidance

**MANAGE**
- Logic Model
- Performance Development Plans
- Work plans
- Job Descriptions

**ANALYZE**
- Management information systems
- Performance Measure Tracking
- HR, IT & Finance Reports
- Customer & employee feedback
- GMAP Report Templates

**RESPOND**
- GMAP Sessions
- Executive Management Meetings
- Advisory Boards

**IMPROVE**
- Process Improvement
- Lean, Six Sigma, etc.
- Business Portal & Permit Streamlining
- Plain Talk
- Performance Audits
- Program Evaluation

**RESULTS!**

**COMMUNICATE RESULTS & LISTEN**
- Communications, including web & outreach
- Plain Talk
- Customer Surveys & constituent groups
Enterprise Risk Management

GOAL: Improve health and safety for all citizens

OBJECTIVE: Implement effective enterprise risk management practices

ACTIVITY:
We implement Enterprise Risk Management (ERM) in state agencies

PERFORMANCE MEASURE:
- Increased Maturity Model Scores in Target Agencies

Output

... so that ...

Agencies can identify, evaluate and mitigate risks by concentrating scarce resources in the areas of most need to reduce losses

PERFORMANCE MEASURES:
- % of agencies that have fully implemented risk analysis and mitigation practices

Immediate Outcome

Degree of Control and Influence

... so that ...

Resources are efficiently used to further program goals

PERFORMANCE MEASURES:
- Risk analysis integrated into agencies’ strategic and budget planning
- Risk register integrated into agency operations

Intermediate Outcome

... so that ...

We reduce deaths, serious injuries and other substantial loss statewide

PERFORMANCE MEASURES:
- % decrease in claims and lawsuits
- % decrease in reported incidents

Ultimate Outcome

We reduce deaths, serious injuries and other substantial loss statewide
How We Met the Challenge

- Purchased ERM training for agency executives
- Developed a flexible 7-Step ERM Method that would work for agencies regardless of their business functions
- Pilot Training Program
- Designed easy-to-use ERM tools
- Taught ERM method to hundreds of state employees in dozens of agencies – so far!
Washington’s Maturity Model

- Using a maturity model tool to assess ERM progress is sound business practice
- ERM Maturity is measured annually in five areas:
  - Fundamentals of Risk Mgt
  - Executive Leadership
  - ERM Integration into Agency Culture
  - Applying ERM Principles
  - ERM Embedded into Agency Strategic Business Operations
- 100+ FTE agencies report Maturity scores to the Governor (GMAP)
This is a portion of a GMAP presentation made to the Governor in 2008.

GMAP is designed to provide the Governor with progress reports on critical performance measures on key agency activities.

ERM is one of the performance measures for Government Efficiency.

Agencies give ERM updates twice annually to GMAP.

Data Source: Agency assessment forms, March 2006 – May 2008
Measuring Our Progress

- The Maturity Model gives a broad overview of ERM Implementation
- 100+ FTE agencies also give detailed descriptions of implementation successes and best practices annually to the Governor
- 3-year roadmap for implementing essential ERM functions

<table>
<thead>
<tr>
<th>2008 ERM Maturity Milestones By Agency Initiative</th>
<th># Agencies Complete</th>
<th>Planned for 2008</th>
<th>Planned for 2009</th>
<th>Planned for 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieved Enterprise Risk Management Maturity Model Level 4 or above</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management responsibility assigned to specific employee.</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management on executive leadership team agenda at least quarterly</td>
<td>20 9 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency Enterprise Risk Management policy in place or in progress</td>
<td>9 12 9 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agency incidents reported centrally and reviewed periodically</td>
<td>26 4 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risks that can prevent achieving program goals are discussed and ranked by severity and frequency (Risk Mapping)</td>
<td>5 15 10 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigation plans are developed when needed for high ranking risks</td>
<td>13 10 5 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where risks are under control, ‘best practices’ that provide control are gathered and shared throughout agency</td>
<td>9 4 9 10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk analysis integrated into agency strategic and budget planning.</td>
<td>11 4 11 6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Where We Are Now

- We provide free:
  - Advanced ERM training
  - Basic ERM training and information
  - Quarterly Risk Forums
    - Ex: e-Discovery
    - Ex: Public Disclosure law
  - New Publications
    - Risk Management Basics
    - Updated Maturity Model
Let’s Review One of our Agency Training Programs
Using the ERM Method

Enterprise Risk Management in Action
Place Your Bets!

- What can we learn from a couple of cards?
- ‘Risk appetite’ varies
  - At play
  - At home
  - In the community
  - At work
- How we respond to risk depends on our tolerance and personal history
- Different risk appetites can cause conflict!
What Is ‘Risk’?

- Most of us have a limited risk vocabulary even though we deal with risk everyday:
  - The yellow light
  - Asking for a raise
  - Noisy neighbors
- ‘Risk’ often has a negative meaning or we equate it with danger
- Most risk assessment happens at ‘gut level’
- …but your gut is often wrong
  - Fear of flying
  - Alligators, snakes and bears, oh my
- We need a better way
ERM Starts With Goals

- Traditional risk management looks at events like car accidents, workers compensation claims, safety violations, lawsuits and other bad stuff to figure out whether we need to change a policy or process to better protect the organization, clients and employees.

- ERM looks at every important goal in an organization (not just accidents or lawsuits) and all the things-bad or good-that could stop you from reaching each goal.

- The ERM method helps you figure out which risks you need to do something about, which you should keep an eye on, and which you can stop worrying about.

- ERM works for any kind of goal
Can We Forget about Tradition?

- ERM doesn’t *replace* traditional risk management activities.
- You have to keep doing everything necessary to:
  - Treat staff, clients & vendors fairly and equitably
  - Keep people safe
  - Respond to claims & lawsuits
  - Be prepared for emergencies
- Sometimes one of these ‘traditional’ areas will need special focus and might then become a new organization goal you assess with the ERM method.
The ERM Method: 7 Simple Steps

1. Clearly state the goal.
2. List everything that could keep you from meeting the goal (the ‘risks’).
3. Evaluate each risk:
   - Choose a likelihood rating from 1-5
   - Choose an impact rating from 1-5
   - Multiply together & ‘Map’
4. Prioritize (Pick the most severe risks)
5. Treat/Mitigate:
   - Avoid
   - Accept & Monitor
   - Transfer
   - Reduce the likelihood
   - Reduce the impact
6. Make a Risk Register that includes:
   - Treatment Plans
   - Measures of success
7. Communicate Results
   - Gather & share ‘best practices’
   - Review & Refine
Step One: State Your Goal

- State in the positive
- Be specific and precise
- Have a time-frame in mind
Step Two: List the Risks

- List everything, good and bad, big and small
- Include everyone
- You may want to involve others, too:
  - Put on staff meeting agendas
  - Send out a survey
  - ‘Subject Matter Experts’
- Don’t be distracted by ‘cures’ right now
Step Three: Evaluate the Risks

- **Likelihood** (How likely is this risk to happen in my time-frame?)
  1. Hardly ever
  2. Once or twice
  3. Often
  4. Frequently
  5. Almost always

- **Impact** (How would it affect my goal if it happened?)
  1. Very little
  2. Minor
  3. Major
  4. Critical
  5. Fatal

It is common to see different words used to describe the scores and even the categories, like ‘Frequency/Severity’ or ‘Likelihood/Consequence’
Step Four: Map the Risks

- Multiply the risk ‘scores’
- Find the risk score on the map
- The most severe risks will fall in the ‘Red Zone’
- Unless you have unlimited resources of people, time and money…pick the most severe risks to work on!

<table>
<thead>
<tr>
<th></th>
<th>1 Very Little</th>
<th>2 Minor</th>
<th>3 Major</th>
<th>4 Critical</th>
<th>5 Fatal</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Almost Always</td>
<td>(5)</td>
<td>(10)</td>
<td>(15)</td>
<td>(20)</td>
<td>(25)</td>
</tr>
<tr>
<td>4 Frequent</td>
<td>(4)</td>
<td>(8)</td>
<td>(12)</td>
<td>(16)</td>
<td>(20)</td>
</tr>
<tr>
<td>3 Often</td>
<td>(3)</td>
<td>(6)</td>
<td>(9)</td>
<td>(12)</td>
<td>(15)</td>
</tr>
<tr>
<td>2 Once or Twice</td>
<td>(2)</td>
<td>(4)</td>
<td>(6)</td>
<td>(8)</td>
<td>(10)</td>
</tr>
<tr>
<td>1 Hardly Ever</td>
<td>(1)</td>
<td>(2)</td>
<td>(3)</td>
<td>(4)</td>
<td>(5)</td>
</tr>
</tbody>
</table>
Step Five: Treat Priority Risks

To treat/mitigate a priority risk:
- Avoid
- Accept & Monitor
- Reduce the Likelihood
- Reduce the Impact
- Transfer

The treatment you choose must:
- Fit the risk appetite of your group
- Reflect the amount of control you have
- Be measurable and time-limited

This directs scarce resources to the risks that really matter.
A Risk Register is a list of priority risks & an overview of how you will handle each.

Start with the goal

List priority risks and include for each:
- Short description of the risk
- Score
- (Some registers include ‘h/m/l’ control level)
- Treatment chosen
- Brief description of treatment plan
- Measure that will show success
- Target dates
- Person responsible (sometimes called the ‘risk owner’)

<table>
<thead>
<tr>
<th>GOAL:</th>
<th>Risk (Briefly describe; include ‘score’)</th>
<th>Risk Treatment (Check type and briefly describe)</th>
<th>How will we know when we succeed? (What are the ‘measures’?)</th>
<th>Target Date</th>
<th>Person Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□ Avoid</td>
<td>□ Avoid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>□ Accept</td>
<td>□ Accept</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>□ Reduce</td>
<td>□ Reduce</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>□ Transfer</td>
<td>□ Transfer</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

□ Avoid
□ Accept
□ Reduce
□ Transfer
Step 6: Work Your Treatment Plan

- Get people involved
- Assess results with your success measures
- Refine your plan
Step 7: Communicate the Results

- Share your successes (‘Best Practices’)
- Review any gaps
- Reassess
- Refine
Let’s Try It: Pick a Summer Goal

1. Lose Weight/Get Fit
2. Dream Vacation
3. Clean Garage
4. Play more golf
5. Fix up the yard
Seven Steps Reminder

1. Fine-tune the goal statement
2. List anything that could keep you from meeting the goal
3. Evaluate using the 5 point scale
   - Likelihood a risk will happen
   - Impact on your goal if it does
4. Prioritize the scored risks
5. Pick a treatment for the worst one
6. Make a treatment plan
7. Set a deadline and tell how you will measure your plan’s success
Let’s Try It For Real

- Use the ERM Method on your goal:
  - **Strategy 2.3.3:** Improve internal communication and collaboration
    - Refine Goal
    - List all the risks to meeting the goal
    - Assess likelihood & impact
    - Prioritize risks
    - Pick a treatment & make a plan
ERM Delivers Real Results

- Helps you refine goals
- Improves communication
- Deploys scarce resources where they will do the most good
- Is repeatable, scalable & defensible
- Time-specific
- Success Oriented
Find Out More

- Sydney Doré, 902-0589
  - Sydney.Dore@ofm.wa.gov
- Kim Haggard, 902-3054
  - Kim.Haggard@ofm.wa.gov
- Drew Zavatsky, 902-9813
  - Drew.Zavatsky@ofm.wa.gov

- Public Risk Management Association (PRIMA): http://www.primacentral.org/
Implementing Enterprise Risk Management in Washington State

Reflections
Is There a ‘Right Way’?

- The right ERM approach is the one that fits the complexity and culture of your group

- **All** methods include structured ways to:
  - Use goals to set context
  - Understand risk appetite/tolerance
  - Identify risks
  - Assess their relative severity
  - Treat/mitigate severe risks
  - Measure performance
Using ‘Categories of Risk’

- Some ERM methods look at goals (COSO uses the term ‘objectives’) and risks by ‘category’ or ‘exposure’.
- The exact categories vary widely:
  - COSO uses four categories: strategic, operational, reporting & compliance
  - Great Britain uses three: external, operational and change (Each of those has 6-10 sub-cATEGORIES like ‘environmental,’ ‘relationships’ and ‘new policies’)
- South Africa uses six: physical & operational, human resource, technical, business continuity & disaster recovery, credit & market risk, and compliance risk
- Also common: categories for reputation, supply chain, or demographics and industry-specific terms like partnerships, profitability, security, etc.
Should You Use Categories?

- Some groups find it easier to talk about risks when they have a structure to get started.
- Others find it too limiting to fit all program goals into categories.
- If you decide to use categories to review your risks:
  - Do some research; find out which categories are commonly used in organizations like yours.
  - Pick categories that are meaningful in your agency and easily understood by everyone.
  - Make sure that using categories will help the process, not slow it down.
  - Remember that categories are just a way to organize. You still need to state your goals for each category.
Where Is ERM Going?

- ‘ERM evolution’- sharing ERM implementation best practices with all agencies
- Increased participation
  - 41 agencies and growing:
    - 32 cabinet agencies >100 FTE
    - 5 smaller/volunteer agencies
    - State Investment Board
    - State Universities
- New training initiative for small agencies
- State Enterprise Risk Register
- National Risk Register?