RISK MANAGEMENT 101 (Short Version)
PARMA CONFERENCE 2015

Rick Buys, ARM
Municipal Pooling Authority
PARMA President, 1999 - 2001

Bonnie Kolesar, ARM
Solano County
PARMA President, 2001-2003

In the past, Risk Management has been treated as a separate function performed by an individual or group, and for the most part, in isolation from the rest of the entity. The Risk Manager reports to a particular department, which varies from entity to entity, makes recommendations, upon which that department head decides whether to act on those recommendations. Risk Management was never integrated into the entity, leaving a poor level of optimization of Risk Management.

Much of the reason for this approach has been that Risk Managers have been viewed as looking only at the downside of risk, leading to a negative view of Risk Managers - people who only know how to say "no." It is critical for us to change that model and view of Risk Management to reach the full benefit that our profession can offer to our entities.

The ARM model has been unable to overcome this deficiency.

I. SOME USEFUL DEFINITIONS:

Risk *- the potential for loss or gain caused by an event or activity (or series) that can affect the entity's achieving its objectives. (The traditional definition of risk is inadequate because it does not consider the potential reward for taking risk.) Taking no action does not eliminate risk, since it is also a risk to decide to take no action.*

Risk Management *- a systematic process to managing risk within the acceptable risk appetite of the entity. The most effective system requires embedding the risk management process throughout all levels of the entity. Embedded into this model are the critical components of judgment, decision-making, communication and documentation.*

Enterprise Risk Management *- a process carried throughout an organization, designed to identify potential events that may affect the achievement of its objectives, in either a positive or negative manner.*

Risk Avoidance *– actions taken to entirely eliminate the possibility of loss.*

Risk Control – *technique of minimizing the frequency or severity of losses with training, safety, and security measures.*

Risk Financing *- achievement of the least-cost coverage of an organization's loss exposures, while ensuring post-loss financial resource availability.*

Risk Tolerance *- willingness of an organization to incur risk to gain future reward.*

Risk Transfer *– transferring liability of an asset or activity to another organization, typically achieved through either contract with an organization or insurance.*

II. IT'S A PROCESS, NOT A FORMULA

Taking on risk requires documentation and analysis of that risk and recognition that the decision to accept that exposure was an informed one through proper deliberation. Every action that creates value also carries risk - risk and value cannot be separated. Risk is a decision driver rather than a consequence of decisions requiring that risk be considered on the front end of every decision to both identify potential threats and to strategically select the risks the entity chooses to take in pursuit of value.

Risk management cannot be implemented with stand-alone initiatives. Rather, it must be built in to the way the organization does business, not bolted on, as a proactive process. This allows for less chance to be blindsided by threats and become more resilient dealing with adversity, while more agile in pursuing opportunity.

This assessment process allows you to identify where "good enough" works versus critical areas where you need best practices to meet expectations.

High level risk management requires proper infrastructure:

- <u>People</u>: Identify, engage, and develop talent to make decisions about risk and risk-related decisions, and give them the tools for that job, through:
    - Role-based training
    - Risk-aligned compensation and rewards
    - Risk-aware culture
- <u>Process</u>: Establish processes for consolidating risk information from different groups, sharing it across the entity and presenting an integrated view to leadership. This will:
    - To improve effectiveness
    - Remove redundancies
    - Improve efficiency
- <u>Technology</u>: To deliver the right type and amount of information to the right people, timely, to help them understand risk associated with certain decisions. Technology delivers high quality, reliable information from dispersed operations to assist in managing risk.

Analysis of an exposure requires consideration that the strategy itself may be flawed due to invalid assumptions. Be prepared to systematically challenge those fundamental assumptions. The keys to watch:

<u>Experience can be misleading</u> - Do we rely upon what has happened in the past, or do we discard them as inapplicable now. (The traditional conservative vs liberal philosophy argument. The key is finding balance between the two.) Watch deeply held beliefs, as they are especially blinding.

<u>Things you know you know, that you don't really know</u> - a particularly fatal flaw. It isn't the things we don't know that get us into trouble.

<u>Thesis-Antithesis-Synthesis tool</u> - the process is:

1) State a proposition upon which success or failure lies (a conventional wisdom or white swan);
2) State the exact opposite, the antithesis or black swan, essentially asking - "What if we are wrong?"
3) Analyze the two positions to identify the assumptions and challenge the assumptions to uncover the most basic, hidden assumptions - the ones no one brings up because they are beyond contesting.

The monitoring phase of the Risk Management Process includes looking for signals of "black swans." Have an early detection system to find them:

- Gather internal and external intelligence.
- Develop networking opportunities with your counterparts and other resources.

III. THE PLAYERS

Maintaining alignment between risk exposures and business strategy requires coordinating the efforts of three levels of risk management responsibility (fig. 2, pg7):

Risk Governance - Board oversight at the top, including strategic decision-making and risk oversight through communication with the executive team on key strategic, operational and compliance risk thresholds, with parameters established in advance as to:

- Quantitative and qualitative analysis of risk rated as high, medium or low on impact, vulnerability & speed of onset.
- Defined risk tolerance thresholds and the controls used to minimize risk.

Risk Infrastructure & Management - the executive team performs management of the people, process & technology by designing, implementing and maintaining the risk management program. In this manner, they set expectations, ensure accountability, engage the Board, and drive change.

Risk Ownership - business units and supporting function groups perform the day-to-day risk process, including the six steps of the risk management process.

Activities across all three levels are integrated in a systematic, enterprise-wide program with a strategic view of risk in all aspects of business management giving leaders a clear view into the challenges and opportunities that risk creates. (fig 3, pg7) Risk management is not viewed as a project but is part of the culture: the way we do business.

A member of the "C-suite" must take a leadership role of risk management (CRO or someone else) to chair the risk group that has authority to escalate significant risks to the RM team or Board as necessary. This individual is not responsible for independent the RM team, so as to challenge RM team actions to the team and the Board.

HR, finance, IT, legal, etc., support departments in their risk program responsibilities. They own their own risk, but support other departments in managing their risks as well. They participate in risk committees and other risk forums.

Internal audit, risk management, compliance, etc., report on the effectiveness to governing bodies and executive management.

They provide this in different roles:

Visionary: assessing the current state and looking ahead to future risks and opportunities.
Dietician: determine if the risk diet matches the appetite.
Aggregator: determining if the entity considers how risks interact and cascade.
Efficiency expert: by eliminating inefficiencies.
Advocate: advocating for resources.
Subject matter resource: providing knowledge and expertise in key risk areas.
Troubleshooter: controlling remediation and design, conducting and interpreting risk assessments.

"*Never tell people how to do things. Tell them what needs to be done and they will surprise you with their ingenuity.*"
--General George S. Patton [just make sure you participate in the process]

IV. SIX CORE FUNCTIONS OF RISK MANAGMENT

The Board & C-suite use a top-down approach of risk at a strategic level, while the rest of the entity use a bottom-up approach to ID and monitor specific risks, escalate concerns to management and generate the data to inform the strategic view. This facilitates the flow of information up, down, and across the entity to manage specific risks while keeping leaders focused at the strategic level.

1. SET HIGH-LEVEL GUIDELINES

Key questions:

- How much risk do we take?
- What kinds of risks?
- How do we define our risk appetite and tolerance?
- Ask where are we, where are we going and how do we get there?

The first step - set high-level guidelines on how to ID, evaluate and communicate about risk - a common set of standards for risk ID and measurement to make the apples-to-apples comparisons to gain a coherent view of risk across the entity, through the following steps:

Establish the risk definition/philosophy - develop a risk philosophy statement that describes the entity's level to which it will seek out, tolerate and/or avoid risk that is recognized throughout the entity. It must also recognize risk-taking as a means to add value, which raises the value of risk management to the entity when the view of risk includes the chance of reward. Example: "*Our entity values risk-taking in its major strategic initiatives and does not tolerate risk taking in non-compliance and violations of business ethics*."

Establish the risk management framework - the entity's basic conceptual structure for how to think about risk, which includes formal definitions of areas of risk that are meaningful to the entity. It must be adaptable to your entity. Frameworks such as COSO, ERM, Turnbull, ISO, ARM and other can help provide structure.

Define the entity's risk appetite - risk philosophy defined into specific guidelines of the acceptable level of risk to the entity. It clearly describes elements considered important and serves as the fundamental standards by which all risks are judged acceptable or unacceptable.

Define risk tolerances - define specific risk tolerances that specify threshold level of risk by incident, in terms that decision-makers use to guide which risks to take or refuse.

Define risk assessment criteria - establish common standards to evaluating risk along three dimensions:
Impact of the risk event (inherent risk)- the extent a risk event would affect the entity without treatment.
Vulnerability to the event (residual risk)- the extent a risk event would affect the entity with treatment.
Speed of onset- time for the risk event to manifest from occurrence to effects becoming felt.
[See Frequency/Vulnerability/Severity Matrix.]

2. DEVELOP A RISK STRATEGY

Developed by the Board and revisited regularly as major factors in the environment change.

Key Questions:

- How valid are our core assumptions underlying our strategy?
- Which strategic options meet our risk appetite?
- What risks must we take to meet our duties?

Setting a strategy entails both the risks of the selected strategy and the execution of that strategy. Two activities should be embedded into the strategy-setting process to help ID unseen risks of the strategy and steps to mitigate them, including developing alternative strategies based on different assumptions

1. Make explicit the assumptions on which the strategy is based. One method to achieve this is:
Thesis-Antithesis-Synthesis Framework (TAS)- to encourage leaders to explicitly state their assumptions underlying a proposed strategy - the "white swans" or event expected to occur. For each assumption, its antithesis is stated - its exact opposite or the "black swans," the unconventional view, unexpected event or improbable circumstance. This forces leaders to ask "What if we are wrong?" The leaders are forced to develop a unified approach synthesizing both the thesis and antithesis into a scenario encompassing both possibilities.

2. Challenge those assumptions to test their validity.
Consider the potential interactions those options might entail to individual strategic choices and to different combinations of choices. Then evaluate the risks associated with each option against the entity's risk appetite.

3. GET TACTICAL WITH RISKS

Risk ID and assessment is done quarterly by a risk committee or when new risks are identified.
Key Questions:
What risks are we taking?
How prepared are we to address those risks?
How would each risk affect our goals?

The process is structured and disciplined, considering input from line managers for their perspective "on the ground." It includes how multiple risks, in combination, may interact to create greater than anticipated exposure.

4. DEVELOP ACTION PLANS
Performed by business units and functions periodically or when a new risk is identified.
Key Questions:
How will we know if a risk is imminent?
How will we respond to risk events?
How do we best allocate our risk management investments?

5. TAKE AN ENTERPRISE-WIDE VIEW (responsibility lies with all)
Key Questions:
What are the top risks?
What are the interactions among those risks ?
How significant are the interactions to the overall risk profile?

Synchronize activities across institutional boundaries so everyone speaks the same language and defines risk the same way. This practice avoids development of departmental **Silos** - miniature ecosystems that complicate communication across the entity. Note however, that silos also represent risk specialization, as part of the critical decision-making process. But specialization requires steps to break down institutional barriers that inhibit collaborative risk management. This is resolved through cross-functional teams that share information, perform joint analyses, & engage in scenario planning. As part of this process, the CRO is not a risk "czar," but a central point of coordination/collaboration.

As part of this enterprise-wide view, each department should maintain responsibility for its performance in risk. Individual departments should view themselves as owning the risk. They identify, measure, monitor, control and report on risk to management, promote risk awareness and prioritize activities.

6. MAINTAIN CONSTANT VIGILANCE (responsibility lies with all throughout the entity)
Key Questions:
How do we monitor internal & external environment for signs that risk is increasing/decreasing?
What are the thresholds for escalation of risks?

An entity must develop effective signal detection and interpretation abilities to alert that risk has changed - both external to the entity and internal performance indicators.

Keep abreast of Key Risk Indicators (KRI's) established by the entity for specific risks. Are there new KRI's? Are some no longer considered KRI's?

V. REPUTATIONAL RISK

Reputation is important across all four major risk areas: **strategic**, **operational**, **financial**, and **compliance**. Managing this exposure focuses on identifying the key drivers of, or impediments to, reputation.

This exposure is often unexpected when only an inside-out perspective (using only inside data) is considered. An outside-in approach helps to ID unexpected developments and spots changes that may be developing since many root-cause events come from outside the entity.

A Reputation Risk Framework
There are three phases to integrate an outside-in perspective:

Discovery - a detailed examination of the current view of strategies, risks and vulnerabilities; finding the "*known-knowns*" and "*known-unknowns*" by a series of in-depth interview with C-suite executives, to ID key stakeholders that provide the outside-in perspective:

- Strategies and their assumptions
- Key industry threats and opportunities
- Major vulnerability points in the entity
- Pressures in the industry
- Weaknesses in recruitment or staffing
- Regulatory and IP exposures

Baseline - Key stakeholders are engaged to assist through a variety of techniques, geared to the audience. Damage occurs much faster now with media and technology. Other tools:

- Searching web dialogue:
    - Blogs
    - Forums
    - Websites
    - Social Media
- Use your employees as sensors - a collective source of front-line intelligence.

The entity can then analyze how the stakeholders view reputational impact, versus management objectives.

Proactive Management of Reputation - three areas of focus:

- **Anticipation**: of threats to strategy and opportunity
    - Know how you would respond to a social media campaign
    - A sensitive internal email is sent to a journalist
    - An offensive video made by one of your employees
- **Analysis**: trends of threats or opportunities
- **Action**: on behaviors to assure successful strategic execution

An entity with a damaging event should turn outward, not inward to protect itself in the marketplace and media. Controlling the exposure and the message is difficult after the damage is done.

Examples:

- Police dept coming under overview of the DOJ or federal judge for 10 years
- Orange County derivative scandal of 1990's
- City of Bell scandal - City Manager, Assistant and 5 Council members all sentenced to prison

FREQUENCY / VULNERABILITY / SEVERITY MATRIX

(A Risk Ranking System)

Focus especially on those risks whose vulnerability has not been addressed. Earth Quake example: whether a building is reinforced or not, or relocated.

FREQUENCY	VULNERABILITY	SEVERITY	TREATMENT

LF LF HV	LV HV LV	LS LS LS	Low Level Exposures: Ignore or Mitigate Internally
HF LF	HV LV	LS HS	Mid Level Exposures: Mitigate Internally or Transfer
LF	HV	HS	High Level Exposure: Transfer or Avoidance
HF HF	HV LV	HS HS	Extremely High Exposures: Avoidance

Severity controls the need to respond, which includes the impact of the loss on the entity. (How bad can it get?)

Vulnerability is the risk remaining after control techniques are applied, also considers the speed of the onset (aka-velocity) of loss (how likely an event will occur and how fast it can hit your entity). This affects how much cash you need on hand to pay for possible losses.

Frequency (aka-probability) compounds the need to control severity or vulnerability. (How often can it get bad?)

THE CRITICAL DECISION MAKING PROCESS

Why do leaders and organizations make poor choices? Examples: Polaroid-Enron-Timex
What techniques and behaviors can leaders use to improve in their entity?
How do you best utilize the diverse expertise, perspectives, and talents of your entity?

Decision-making occurs at three levels: <u>individual</u>, <u>group</u>, and <u>organizational</u>.

INDIVIDUAL LEVEL DECISION MAKING

We typically do not examine every possible alternative or collect all possible data when making choices. Instead, we draw on our experience or apply rules of thumb. That leads to "*cognitive bias***"** decision traps that lead to systematic mistakes in making choices.
At the individual level, the mind plays tricks on us:

- We make biased judgments due to "*cognitive bias," "over confidence" or the "sunk cost effect*."
- Intuition can lead to inaccurately match current problems to patterns from our past.

GROUP LEVEL DECISION MAKING

Teams often do not employ the diverse talents and knowledge of the individuals effectively. Problems like "*group-think*" arise, which can suppress dissenting views.
At the group level, teams do not always make better decisions than individuals:

- Groups offer pooling the intellect, expertise, and perspectives of many people.
- That diversity can lead to better decisions.
- But many groups fail to realize the synergy, making decisions inferior to those of an individual.
- This is because groups encounter the social pressures of conformity.

ORGANIZATION LEVEL DECISION MAKING

An organization's structure, systems, and culture shape the behavior of individuals and teams, which can result in multiple, small decision failures forming a chain of events leading to a catastrophe.
At the organizational level, structure, systems, and culture shape the decisions:

- Our environment shapes how we think, interact with others, and make judgments.
- Organizational forces can distort the information, interpretations of data, and communication.

PROBLEMS FACED IN HIGH-RISK DECISIONS

Leaders can improve their ability to make high-stakes decisions.

- In most cases, intellectual ability does not make the difference.
- The difference is usually in the social, emotional, and political dynamics of decision-making.

Understand how decisions are made in organizations to improve decision-making skills.

<u>Myth</u>: Decisions are made in the room.

- Much of the work occurs in private conversations or sub-groups, before the meeting even begins.
- Formal staff meetings often simply ratify decisions that have already made.

<u>Myth</u>: Decisions are largely intellectual exercises.

- High-stakes decisions involve complex social, emotional, and political processes.
- Social pressure for conformity and desire for belonging can affect and distort the process.
- Emotions can either motivate us or paralyze us in making important decisions.
- Coalition building, lobbying, and bargaining play important roles in organizational decision-making.

<u>Myth</u>: Managers analyze and then decide.

- Decisions are frequently made before managers define problems or analyze alternatives.
- Sometimes, solutions go in search of problems to solve.
- Managers often decide on a course of action and then ask their team to analyze the problem, to serve as a tool of persuasion for their decision.

COMMON TRAPS THAT AFFECT CRITICAL DECISION MAKING

A. **"*Cognitive Bias*"** **-** adopting certain rules of thumb or other shortcuts to make choices more efficiently.

B. ***"Over-confidence bias*"** **-** overconfidence in our own judgments.

C. ***"Sunk-cost effect*" –** continued commitment to a decision because of prior investments of time, money, or other resources, instead of recognizing the eroding benefits of the proposal.

D. "***Recency effect*" -** over-confidence based on recent results and under-estimating the odds of failure.

E. **"*Confirmation bias*"** - over relying on information that supports our existing views, downplaying contrary information.

RESOURCES PAGE

- PARMA Website www.parma.com
- Networking among your peers (at PARMA and other opportunities)
- CAJPA http://www.cajpa.org/default.aspx - California public entity pooling information.
- www.primacentral.org - PRIMA Website
- Local Government Institute's Risk Management and Loss Control Manual (253-565-6253)
- http://www.ieatraining.com Insurance Education Association – online classes in ARM & RMPE (Associate in Risk Management, and Risk Management for Public Entities
- Why Great Leadrs Don't Takes Yes for an Answer: Managing for Conflict and Consesus, Michael Roberto
- Get to know your broker!
- Develop relationships/partnerships with similar agencies.