Part 2 Kick-starting the Dialogue on Risk

by Rick Funston and Randy Miller, May 17, 2014

Introduction

The first article in this series "ERM in Public Retirement Systems" described a number of risk scenarios; common questions raised by boards about their system's preparedness; the role of the ERM director or CRO; the differences between risk oversight and risk management, the responsibilities of risk owners and operators; the differences between reasonable assurance and independent reassurance; maintaining the balance between focus on performance and/or process; and the importance of risk dialogue not just reports.

This second article describes how to kick-start the dialogue about value and risk between the board and the executive. We suggest it begins by asking the executive to answer five fundamental questions:

1. What are the major risks to our system?
2. Who is responsible for managing those risks?
3. How prepared are we to prevent or respond to major risks?
4. What can we do to practically reduce any unacceptable exposures given our limited resources?
5. How does the board know your answers are reliable?

But before we talk about the specific risks to your system, it is important to understand what is meant by risk in general. The answer too often depends on who you ask. Those with deep specialist expertise naturally develop their own language. Actuaries may define risk as the frequency and severity of losses and the correlations between contracts. Investment operations may see risk as unexpected variation; HR may see risk as loss of key personnel, Legal may see risk as the potential for litigation; while others may see risk as anything that stands in the way of the achievement of an objective.

It will likely take some time for your system to develop a common understanding and agreement on risk since it is a migration or evolution from divergent specialist perspectives. It is unreasonable to expect, after years within a specialization in which people typically understand and refer to risk in a certain way, that the day following the ERM launch, they will have completely changed their understanding. This is why the risk dialogue between the board and the executive is so important and should not be rushed.

These issues cannot be resolved all at once but form the basis of developing a shared understanding, acceptance and commitment over time through continuing dialogue. Risk and the potential for profit or return are also related to uncertainty. Greater uncertainty creates greater risk of loss and also greater potential returns. For this reason, the discussion of value and risk should never be separated.

1. What are the major risks to our system?

A major risk occurrence can be a single event or a series of events that negatively affect your system. They may even affect your mandate and your ability to operate. They also usually happen a lot faster than you ever thought they would. So what are the major types of risk intrinsic to your system? Consider the acronym **FLOORS** as a way to begin the identification of risk.

Financial / Investment risk

The biggest investment risks for a pension fund lie in its asset allocation and its choice of investment managers and styles. What are the return expectations? Who sets them? What are the consequences if those expectations are too high or too low? Do assets match liabilities? Most systems have unfunded liabilities. What is the plan to close the gap? What are the risks of risk aversion or swinging for the fences?

Legal / Regulatory risk

Often the biggest legal risk lies in the potential misalignment of fiduciary duties and authorities. Do authorities match responsibilities? While there has been a steady migration toward greater investment autonomy, does your system have sufficient control over operational budgets and personnel matters? Another risk is non-compliance with laws and regulations.

Operational risk

Operational risk is unwanted variability caused by people, processes, systems and external factors. Do operational capabilities match investment strategies? Does your system have the right number of people in place in each of its key functions? Does it have the right information systems to support effective and timely decision-making? How long can it go without those key people or systems? How robust are due diligence policies and procedures? Do you adequately protect your data?

Organizational risk

Is there a clear single point of overall executive accountability? Are the rates of turnover acceptable? Is the organization capable of attracting and retaining the skills it needs? Is there key person risk? Are you properly training and cross-training your people?

Reputational / Stakeholder risk

As the old saying goes “Reputation is gained in inches per year and lost in feet per second”. Reputation is the consequence of an organization’s ability or inability to manage its risks and deliver value. It is how people perceive you. In public retirement systems, reputational risk is often associated with other risks such as failure to manage compliance, conflicts of interest, front-running or operational failures.

Another related reputational risk is a lack of stakeholder understanding and support of the system's goals and strategies. The more complex its investment strategy, the more difficult it may be to sustain key stakeholder understanding. Key stakeholders include the system's beneficiaries and the legislature - among others. To the extent that the system is dependent upon the goodwill and understanding of the Legislature, how good are the relations and understanding? Is there a proactive stakeholder communications plan? How confident are stakeholders in your ability to deliver?

Strategic risk

The biggest source of strategic risk lies in the assumptions which underpin your investment, organizational and benefit administration strategies. Are investment beliefs and capital market assumptions explicit? Have they been challenged? Are there mechanisms in place to detect if your assumptions ought to be changing in response to a changing environment? Remember the not so distant assumption that the national price of housing in the U.S. would continue to rise indefinitely. Below are some examples of other strategic assumptions:

- Defined benefit programs are here to stay and so are existing benefit levels
- There is a private equity risk premium
- The best measure of fund performance is relative to its benchmarks
- Expected rates of return are realistic
- The cost of active fund management is worth it

Risk Owners and Operators

Once you have identified a risk, who owns that risk? A risk owner is the executive (or in some cases, executives) responsible for the assessment, mitigation, monitoring and reporting of the exposure associated with an identified risk. The executive risk owner is responsible for developing capable people, policies, processes and systems to assess, manage, monitor and report on value and risk. The ERM program is not a risk owner if its goal is to provide support and independent reassurance. See the first article for further discussion of the differences.

In most cases, the appropriate risk owner should be obvious by their position, e.g., the Chief Investment Officer for investment risks. In other cases, the CEO or Executive Director may need to assign responsibility. Sometimes, it is the board that is responsible for risk management such as asset allocation, or the recruitment, selection, evaluation, compensation and termination of the chief executive. Board vs. executive responsibilities for risk management should be clearly identified as part of its powers reserved and in the delegations of authority.

To the extent that a committee of the board has oversight responsibility for a risk domain, it should receive the relevant reports. If there is a Risk Committee of the board, its role should be that of aggregating and understanding inter-dependencies and ensuring there are capable people, processes and systems in place. For example, HR and IT issues may affect the ability of the Investment Office to further develop in-house investment management capabilities.

Risk operators are the people responsible for operating a process in compliance with laws and regulations and in conformance with established policies and procedures as well as identifying needed improvements. Operators, in turn, need manageable workloads, clear policies and procedures, appropriate training and supervision.

Executive risk owners should then be accountable to answer the remaining questions:

3. How prepared are we to prevent or respond to these risks?
4. What can we do to practically reduce any unacceptable exposures given our limited resources?
5. How does the board know your answers are reliable?

Establishing the risk owner for each identified risk is a critical early step in the successful deployment of an ERM process. By quickly establishing a single point of accountability for the reliability of assurances about the effectiveness of risk mitigation, the stage is set to provide support and assistance to risk owners in developing a common understanding with the board. This usually entails developing a common language of risk, a common process and common tools. Of course, these take time.

This will help risk owners not only coordinate their efforts but also to present a coherent perspective to the board. This requires their agreement on the definitions of various risks, the criteria to be used to assess risk (e.g., how big is big?), an integrated way to present exposures and to provide reasonable assurance. However, the pathway to agreement begins with establishing executive accountability.

This way the ERM process is much better positioned to assist and support executives, rather than be perceived as an added burden to their already heavy workloads or a takeover of their risk management responsibilities. The goal is to make the approach to risk management common across the system where it makes sense and not just for its own sake. This is discussed in the next article in this series "Developing a Common Understanding".

About the authors. Rick Funston is the Managing Partner of Funston Advisory Services LLC which specializes in governance, strategy, risk and compliance. He was formerly the National Practice Leader for Deloitte's Governance and Risk Oversight Services. He is the principal author of 'Surviving and Thriving in Uncertainty: Creating the Risk intelligent Enterprise" Wiley and Sons, 2010.

Randy Miller is a Principal of Funston Advisory Services LLC and former senior consulting partner with Deloitte for 27 years with extensive experience in strategy, benchmarking and operations improvement.

