4 Enterprise-Deep Risk Management

By Rick Funston and Randy Miller, May 25, 2014

Introduction

Typically people talk about enterprise-wide risk management and how to involve the senior executives and the board in identifying, managing and overseeing risks across the organization. But there is also real value in making it enterprise-deep.

Enterprise-deep risk management requires building risk intelligent management into the culture of your system and the ways it operates every day rather than trying to just bolt it on as an after-thought. Risk intelligent management is about taking the time to understand the risks that must be successfully understood, prevented where possible or managed to accomplish your organization’s goals.

Risk intelligent management is, of course, about more than just risk assessments. It includes prevention, detection, correction and on-going monitoring. Unfortunately, many organizations tend to focus much of their time on getting their risk assessment process up and running and less on actual risk management.

The following article describes some of the building blocks to creating a risk intelligent culture and several policies and tools that can help you rapidly deploy risk intelligent management into your system to make it enterprise-deep.

Creating a Risk Intelligent Culture

First, let’s talk about the importance of “tone at the top” and culture. A culture is often defined by its language and its system of shared beliefs, attitudes and values. The last article in this series described a way to develop a common understanding and language of risk. Recall that risk was defined as the potential for failure that results in loss, harm or missed opportunity...
including the risk of inaction. Failure is an unacceptable difference between actual and expected performance. Operational risk is the potential for unwanted or unacceptable variation in performance caused by people, policies and processes, systems or external factors.

With this in mind, a very important role of leadership is to develop shared beliefs, attitudes and values about risk/failure and reward. Risk intelligent leadership understands that calculated risks need to be taken to increase value; deliver quality services; achieve expected rates of return; and to continuously improve. They also know why it is important to avoid risks that offer no reward to the retirement system and its beneficiaries such as non-compliance, conflicts of interest and operational failures.

Risk (the potential for failure) needs to be taken very seriously and not as a mere “check the box” exercise. The riskier the initiative, the more thoughtfully the risk (i.e., the potential for failure) needs to be considered. Professionals who put their lives on the line demand thorough preparation. Whether it is the brave men and women who defend our country, race drivers, astronauts, mountain climbers or stunt men and women, the riskier it is, the more preparation, training, rehearsal, and discipline become essential to improve chances of survival and success. Otherwise, folks may find themselves uttering the same last words as a daredevil who without preparation jumps off a cliff saying “watch this”.

Values, beliefs and attitudes toward risk begin with the behavior of the board and the senior executives and are reflected in practices and policies toward risk and reward. For example, are the bearers of bad news “shot” or “appreciated”? Is there appropriate training and are there proper tools for both prevention and correction? Is there a commitment to thoroughly assess in advance how a major initiative might fail? Is there a requirement to review any risk occurrences / failures after they occur to accelerate learning and prevent reoccurrence? Are people provided with the proper training and tools?

Second, there is also a “tone at the middle and bottom” of the organization. Getting most people to constructively discuss failure (potential or actual) is difficult. Most people prefer to be optimistic and many recite the popular saying “failure is not an option”. But frankly the potential for failure is a reality and simply putting on rose colored glasses does not change that reality, only the perception of it. Neither does turning a blind eye to potential or existing problems.

As Mark Twain once said “Denial ain’t just a river in Egypt.” Even the Chief Risk Officer (CRO) or Director of ERM are often in a tough position. They are often charged with raising the possibility of what could go wrong so it’s hard to not to be seen as a perpetually negative “Dr. No.”
Third, a constructive discussion of risk often requires a cultural shift especially if the organization is risk averse and there is fear of failure and blame. Fear fosters unwillingness to change or innovate and usually stems from fear of recrimination for any failure. The philosophy has to be to “fix the problem not the blame”. Blame should be reserved for those situations where there was a deliberate attempt to cover up or ignore a potential or actual failure but not for identifying it.

Risk aversion generates inertia and unwillingness to take calculated risks and ever increasing bureaucracy. This is why organizations need to become risk intelligent and learn how and when to take calculated risks and when to avoid them.

Fourth, risk management is often seen as something separate and apart from the way the organization runs its business. Too often risk and its intelligent management are things someone thinks about after their day job is done rather than as part of the way they think about their job.

The ‘tone from the top’ and the cultural shift toward risk needs to start with the board and executives to encourage intelligent and calculated risk taking not just risk aversion or “swinging for the fences” without proper forethought. For these reasons, risk appetite and risk tolerance policies are critical to creating and sustaining a risk intelligent culture at the middle and bottom of the organization but also needs to be deployed throughout the breadth and depth of the organization.

**Live and Learn**

As we demonstrated in the last article “Developing a Common Understanding”, as long as you choose to be in a particular business or service system, risk can never be eliminated. Certain risks (intrinsic risks) just come with the territory. There is also a point of diminishing returns beyond which further investment in risk mitigation will not be cost effective.

Obviously, organizations should make every reasonable effort to prevent a risk occurrence but there is no such thing as perfect prevention. When risks/failures do occur, as they inevitably will, there needs to be a way to analyze and learn from them.

Some people call experience the ability to survive a failure and live to learn from it. Thomas Edison, when speaking of his efforts to create the first electric light bulb, said “I have not failed. I've just found 10,000 ways that won't work.” We also typically learn more from failures than we do from success. Bill Gates once said “Success is a lousy teacher. It seduces smart people into thinking that they can’t fail.”
Training and Education

Training and education should begin with the Board and executives. What is their role in risk oversight vs. risk management? What does it mean to be risk intelligent? How should they think about risk and reward? What should they expect from enterprise-wide and enterprise-deep risk management? This will help to develop a common understanding and language of risk.

Describing a process view of the retirement system can be highly valuable way to improve how the board understands how the system works. It makes it also easier to describe how value is created or delivered and how and where can it fail and thus where risks exist. For many people, risk remains an abstract concept until people can see where it exists in the system and understand its effects.

See Chart 1 below for a high level process description of an integrated retirement system. Depending on their mandate, public retirement systems can have as many as seven macro processes or as few as two:

Chart 1 – Retirement System Macro Processes


Each of these macro processes is comprised of sub-processes. Chart 2 below provides an example high-level description for one of these sub-processes:
Risk assessments can then be overlaid on the sub-process model to provide a dashboard to help visualize the risk. In the example shown above, certain sub-processes are rated as high or medium risk of failure.

**Risk Intelligent Policies and Tools**

Together with a common understanding and language, risk intelligent management requires policies and tools. Two of the first policies of any ERM program should require 1) advance risk assessment of major initiatives to identify potential program, system and process failures and 2) follow-up reviews and analyses of root causes of any actual failures to prevent reoccurrence and improve risk management.

For example, when CalPERS began their ERM program in 2010, one of the first things they did was to require executive risk owners to complete risk assessments of all major initiatives. Whenever a major program, process or policy initiative is presented to the executive and/or the board, it must be accompanied by a risk assessment. ERM personnel were also there to help with the assessment process and to provide independent reassurance about the robustness and reliability of the risk assessment.

These two requirements will also help inform the development of policies regarding risk appetite and risk tolerance.
A Risk Intelligent Toolkit

In addition to clear policies and appropriate training, it is important that there also be tools to support building risk intelligent management capabilities. There are two key tools that public retirement systems can use to identify, analyze and then mitigate risks:

1. Failure Modes and Effects Analysis (FMEA) an identification and prevention tool
2. Root Cause Analysis (RCA) a correction tool.

Both of these tools are adapted from Total Quality / Six Sigma programs and have proven highly valuable in risk management.1

1. Failure Modes and Effects Analysis (FMEA)

FMEA is a very useful tool that was originally developed by NASA to proactively assess risk, identify potential causes of failure and prevent them before they occurred. It is most often used in new process or program design and requires designers to answer five basic questions:

   Step 1: What are the steps in the process or program?
   Step 2: What could cause it to fail?
   Step 3: What would be the effects of the failure?
   Step 4: What can be done to prevent failure?
   Step 5: Is the residual risk acceptable?

2. RCA (Root Cause Analysis)

The FMEA tool is one way to prevent failure. Unfortunately, there is no such thing as perfect prevention. Failures will inevitably occur. The key is to quickly detect, correct and learn from them. Learning requires quick feedback without assigning blame.

Another way is to require that a Root Cause Analysis be completed for all major risk occurrences (failures). Once a failure has occurred, Root Cause Analysis can help to identify and correct causes and prevent reoccurrence by asking:

---

**Step 1:** Why did it fail?
**Step 2:** What caused it to fail?
**Step 3:** What can be done to eliminate this cause and prevent future failure?

It is the mirror image of FMEA. See Chart 3 below.

**Chart 3. FMEA and RCA**

For more information on FMEA and RCA, visit our website at [www.funstonadv.com](http://www.funstonadv.com).

**Conclusion:**

This article described a number of ways to build the foundation for a risk intelligent culture. It also described several tools to help visualize risks that can be of help ranging from the board to risk operators throughout the system. Requiring a risk assessment as part of every major initiative can help to prevent risks and requiring a Root Cause Analysis after a major failure can help to prevent reoccurrence.

With a common understanding of risk, a clear statement of beliefs to guide decision-making and the right policies and tools, public retirement systems can more rapidly deploy an effective enterprise-deep risk management process. More information about risk intelligence in public retirement systems is available on our website at [www.funstonadv.com](http://www.funstonadv.com).

The next article in this series discusses strategic risk and the role of the board.
About the authors. Rick Funston is the Managing Partner of Funston Advisory Services LLC which specializes in governance, strategy, and risk intelligence. Rick 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.

www.funstonadv.com