

# Enterprise Risk Management – How to (finally) Get Value Out of All of Your Efforts

by John Hurlock

In the recent movie, *The Hangover*, four friends head to Las Vegas because one of them is getting married. The next day they wake up and discover they have lost the groom, among other things (and even found some things they weren't expecting). The question they ask themselves throughout the movie is, "What did we do last night and how did we wind up where we are?"

With respect to Enterprise Risk Management (ERM), many bankers (and Board members) are asking themselves the equivalent of the same question. With all of the money and time we have invested in risk management over the last ten years, how did we wind up where we are? Why are we experiencing the losses we are experiencing and how come our program didn't let us know early on what we were going to face so we could have taken appropriate actions to avoid the losses, pain and suffering we are now experiencing?

Bankers, by and large, have endeavored to build good, solid risk management programs to mitigate their exposure to loss. Some bankers have been enthusiastic about building a robust ERM program while others have been dragged along by the regulators, with the majority of bankers taking actions to appropriately protect their financial institution. But again, protect them from what?

So what went wrong, if, indeed, anything did go wrong? And what do we need to do now, assuming we are going to survive? Because I don't believe any of us want to go through the same pain and agony we are currently facing.

In this white paper we will explore why we are where we are in the world of ERM and what actions we need to take now to prepare our-

selves for the future. We will discuss some of the events that have unfolded and offer you a different way to view your organization. We call this the Outside-In, Inside-Out, Top-down Bottom-Up approach, an approach we believe will have you looking at your bank differently while giving you the opportunity to balance risk and reward.

## What is ERM?

- ERM - The identification, quantification and monitoring of the downside risks faced by the financial institution enabling the development of a mitigation program that reduces bank specific risk and provides analytic predictive information on systemic risk.
  - Identification
  - Quantification
  - Monitoring
  - Mitigation
  - Reduce Bank Specific Risk
  - Predictive Information on Systemic Risk
- This enables the Bank to take early actions to reduce loss and exposure.
- Reduces uncertainty regarding Bank performance.

## The Background – The Development of ERM

ERM (and the newly coined term Governance Risk and Compliance (GRC)) is the end result of almost 40 years of formal risk management development in banking. The initial focus (in

the 60s) was on absolute loss and the use of insurance products to mitigate the loss to the organization. In the 70s, we had a new set of risks appear. Foreign Exchange risk, the introduction of the options market, inflation and the subsequent high interest rates are just a few of the risks bankers came face to face with then. During this period of time the Office of the Controller of the Currency (OCC) introduced a formal loan grading system, which most banks still use today. The 80s began with the introduction of the Depository Institution Deregulation and Monetary Control Act of 1980, which in many respects laid the foundation for the current banking environment. The 80s also saw the formal development of the compliance function in response to the consumer banking laws that had been enacted earlier. And, of course, we also saw the first widespread use of asset liability management (ALM) models to manage interest rate risk, as well as the introduction of Basel I (1988), the risk-based capital guidelines currently applied in the US.

Fast forwarding through the 90s towards the end of the 90s, the focus shifts to a newly defined risk category: Operational Risk. This shift came about as the result of some significant corporate failures such as Barings and Enron, to name a few. In addition, computer technology and the financial institution industry's heavy reliance on it exposed everyone to new and unforeseen risks.

For the last ten years, financial institutions have primarily focused on building out the operational risk part of ERM. Laws such as Sarbanes Oxley, Gramm, Leach, Bliley and the Bank Secrecy Act have been the principal drivers behind their focus. Besides these laws, don't forget the regulators were equally stressing risk-based requirements for developing Business Continuity Plans and Vendor Management programs.

The technology tools that are now being touted as ERM or GRC tools all have their roots in operational risk. The technology is more advanced but still is rooted in Operational Risk. Many were introduced as archiving and reporting software packages to document the compliance

efforts for Sarbanes Oxley. These tools were then adopted as operational risk management software, then on to enterprise risk management and now are labeled governance, risk and compliance software. Each iteration of the tools though has the foundation of archiving and reporting.

Managing risk is much more than an archiving and reporting activity, however. It involves peering into the current state of affairs and trying to predict the future. As much of the banking world has discovered, the focus on operational risk did very little to prepare for the systemic tsunami that struck with a vengeance. Before we move on to ERM, a review of what is risk is presented.

### **What is Risk?**

First and foremost, risk is always in the future. This sounds like a simple description (or blindly obvious observation, as one colleague puts it) and it is. Sometimes, however, the past gets confused for the future. For example, a study was done after Hurricane Katrina decimated New Orleans to determine why people remained in the city even after being urged to evacuate. A common thread among those who stayed was that they had survived 1969's Hurricane Camille. The people used Camille as their basis for the impending Katrina. In banking we saw this same kind of blind spot in our predictions for loan performance. Moving from 80% to 90% loan-to-value (LTV) on residential real estate and then on to 100+ percent was based on the default experiences with these loans as the LTV climbed. When the recession hit and people could no longer refinance their way out of default, default became the only option.

A second important part of the definition of risk are the concepts of probability and uncertainty (in loan portfolio management these are often referred to as expected loss (EL) and unexpected loss (UL)). The focus on probability has far outweighed the amount of uncertainty that goes along with the probability. The classic example is that of the 100 year flood that strikes three times in ten years. While the probability

could remain at 1 percent, the uncertainty associated with it is really much higher. Uncertainty can change over time, far more quickly than probability (because probability is mostly based on historical observations). The price of something, for example, the price of a loan or investment, should reflect both of these components. The plummeting of banks' stock prices in 2007-2008 and the inability of bankers to raise capital really demonstrated the immediate effect uncertainty can have on an organization. It was not until the stress tests were performed in 2009 did the level of uncertainty decrease and the market began to stabilize. As the Wall Street Journal reported this past August, Treasury Secretary Geithner's announcement of the stress testing program had an immediate and positive effect on the stock price of 18 of the 19 financial institutions (the 19th is private and does not trade).

The third component of risk is the ability to define and measure it. This is the quantitative side of the story. If risk isn't defined and measured, then the programs you develop to mitigate risk have a very poor foundation upon which they are built. Risk can be very subjective and without solid definition and measurement activities, the wrong emphasis can be placed.

You don't have to think too hard to come up with a glaring example: the recent Madoff Ponzi scheme had so much weight placed on Mr. Madoff's reputation that obvious signs of malfeasance were overlooked. As a result, almost \$50 billion was lost because of fictitious investments.

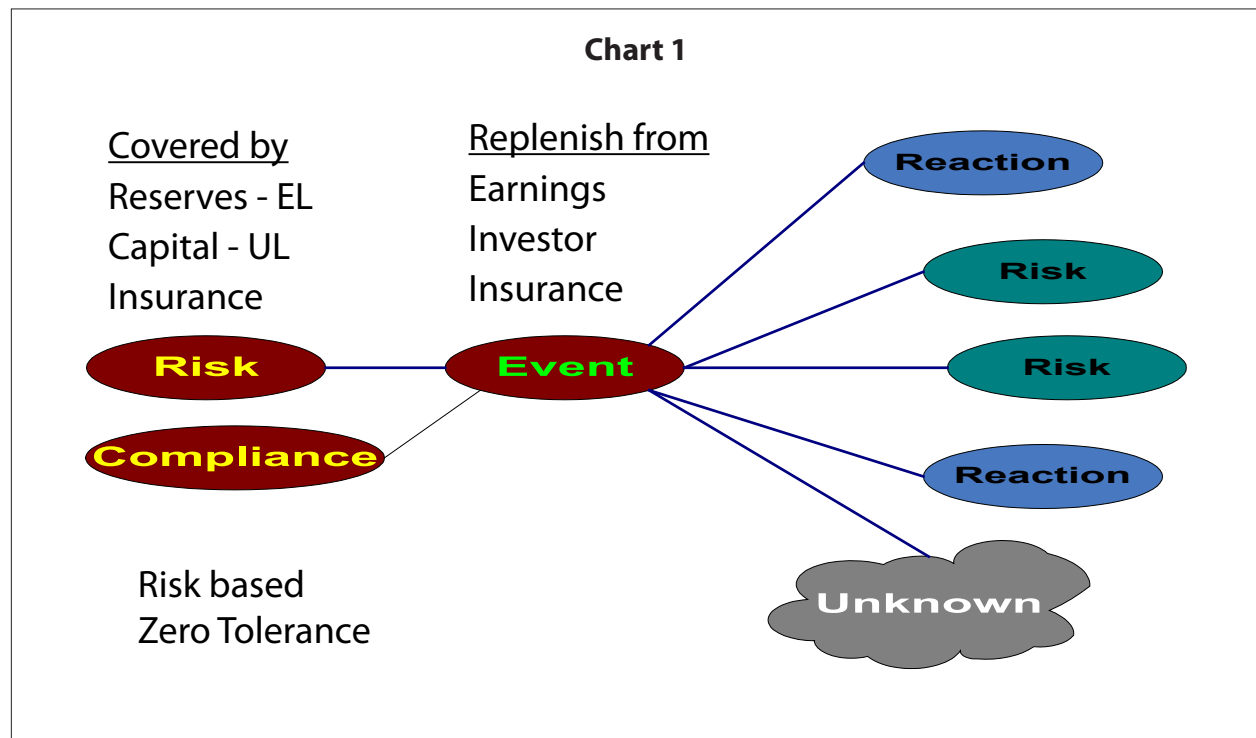
The fourth component of risk is taking action. The goal is to exit an escalating event before everyone else. Mr. Rockefeller once said, when asked how he became so wealthy, "I left the last 10% for everyone else." If you look back at the current crisis, when would have been the appropriate time to exit sub-prime lending for your organization?

Chart 1 below shows how a risk turns into an event and the "offspring" of the event.

To summarize, risk is always a future based event that has two components, probability and uncertainty, which need to be defined and measured before the risk can be managed and from which actions should be taken to mitigate the bank's exposure. Now on to ERM.

**ERM – the Past**

The problem and the reason why some ERM programs didn't provide the proper set of indicators to financial institutions centered on the way the risks were managed. Instead of



managing bank wide the risks were segregated into silos—credit, market, interest rate, and operational risk. Enterprise Risk Management or ERM is meant to be just that, an enterprise activity. The goal of any ERM approach is to consolidate the risks the bank faces and provide information, across business line boundaries. The expected outcome is a recognition of material risk exposures for which risk mitigation plans may be developed. Let's be clear though, some ERM programs worked as anticipated—they did point out the escalating risks and management took steps to mitigate the impact on the bank resulting in missing the storm.

**Case in point:** going back to 2007, interest rates began to rise as a result of inflation fears. Many banks were expecting this to happen and had positioned themselves to be asset sensitive where assets would reprice faster than liabilities. So, from an asset liability management perspective, the bank was well positioned. Digging into the credit side of the house however would have revealed a portfolio of loans that would not be repaid at higher interest rates because the borrower was strapped. The speed at which the loans had been booked meant there was most likely some operational deficiencies in the loan files such as outdated financials or incorrect lien perfection. Looking into the investment side would have found credit risk embedded in various mortgage-backed instruments. And finally, many banks had shifted their loan portfolio mix and were now overweighted (a nice way of saying they had a concentration) in real estate—backed loans. As the recession hit, instead of being well diversified which would have resulted in minor pain (everyone suffers in a recession), the banks found themselves with significant exposures in both the loan and investment portfolios. The rest, as they say, is history.

### **ERM – The Retooled Approach**

ERM in many financial institutions is in need of a makeover. The starting point for this makeover should be a critical assessment of the current state of the bank's overall risk manage-

ment program and efforts, which brings us to the Outside In, Inside Out, Top Down, Bottom Up approach.

### **Expanded View of ERM – Adding to the Top-Down Bottom-Up Approach**

Top-Down Bottom-Up has been a mantra in risk for a number of years. Top-Down refers to the “tone at the top”. In other words, it indicates the support and directives given by the Board of Directors and Executive Management to the risk program. This is extremely important for any initiative, and especially for risk management. If the Board and Executive Management don't accept and support an ERM program, it is likely to fail and, in some cases, create more risk for the bank. Bottom-Up refers to the building of the program by the people who understand it the best: the line managers, supervisors, auditors and the like, all who are very close to the production process.

Now it is time to add in two important pieces which are added on before the Top-Down Bottom-Up components. They are Outside-In and Inside-Out. These two perspectives will help you define your ERM program.

#### **Outside-In**

Outside-In refers to the way your bank is perceived by investors, regulators, depositors, borrowers and anyone else who has a vested interest in your financial institution. Banks are supposed to be profit making organizations and provide a return to the people who put in the capital. This return has a risk and return component and is dependent on the decision making by the bankers who run it.

The Outside-In information comes from all of the information that is available to this audience. The best place to start with this is at the balance sheet. The deployment of capital and deposits dictate the type of return the investor can expect. In analyzing the current economic climate and how banks have wound up with issues, I have found time and time again that the banks have shifted their balance sheets and increased their concentrations in the portfolios where they now have the most problems. To

analyze this, I went back to 2004, generally considered a strong year for banks. I compared the portfolio at that time with the current bank structure and then posed the question, "How would the bank look if it had the same portfolio mix as 2004 but at its current asset size?" One bank I recently analyzed had increased their commercial real estate exposure by 10% since 2004, leaving them with over 60% of the loan portfolio in commercial real estate. This was done at the expense of the consumer and commercial portfolios, which shrunk as a percentage of outstanding loans. This bank has over \$15 million in additional past dues and non-accrual loans because of the shift in the balance sheet structure. As was said earlier, in a recession, everyone will feel some pain. A bank that is not well diversified and has concentrations in the suffering loan sectors will experience far more pain in their loan portfolio.

The information this provides, in conjunction with capital levels, enables an outsider to look at the bank and see if it is more risky than it was during a strong year. Think of it as a sort of stress test on the balance sheet.

### **Inside-Out**

Now, let's move on to Inside-Out. Inside-Out refers to how the bank wants to be perceived by the market. Do the results from the Outside-In reflect the intent of the Board and Executive Management? Or has the portfolio slipped to a riskier structure without anyone really understanding how the bank's exposure to loss had changed? This information is gathered by presenting the outside view to the bank and facilitating a discussion around the information. Another bank, for example, had an 800% increase in off balance sheet exposure by growing their Home Equity Lines of Credit. Executive management knew they had been successful in this arena. They hadn't really looked at the exposure of the bank if all of these lines had been drawn down along with significant increase in default levels. In short, the gap between the outsider's view and the insider's view is where a significant portion of the risk sits. And it is a gap that needs to be closed.

With this information, the Top-Down Bottom-Up approach to building the ERM becomes much more effective. Transparency is added as the bank now understands its risk profile, agrees with the structure, ensures there is sufficient capital to support the structure, and then is managed to maximize the risk/return tradeoff.

Last but not least, COSO's (Committee on Sponsoring Organizations) guidance and frameworks are an integral part of the Top-Down-Bottom-Up component of ERM. The framework they developed is an integrated framework used for reporting on internal control systems and financial reporting. Financial institutions use the integrated approach to determine whether objectives are met in three areas:

- 1) the effectiveness and efficiency of bank operations,
- 2) the reliability of financial reporting; and
- 3) compliance with applicable laws and regulations.

One primary goal of the framework is that you focus on the current behavior of your organization, making sure that what is stated in your organization's policies and procedures actually happens and that there are controls in place and functioning to ensure that your objectives are being met. To back track for a minute, it's the Outside-in-Inside Out initiative, with support from Senior Management and the Board of Directors, that propels the framework into motion. But COSO is not the end all.

Of course it is more complicated than this. Since a bank is a dynamic organization with constantly changing needs and demands from the marketplace, the program has to be actively managed. It is the addition of the Outside-In Inside-Out pieces that will enable the financial institution to mitigate its losses during the downturn and take advantage of opportunities in the upturn. Coupled with the work already done for Operational Risk, the bank can make the ERM program truly enterprise wide.

For more information go to [www.smslp.com](http://www.smslp.com) or call 1.800.477.1772. ■



**John Hurlock**

*Director, Consulting Services, Sheshunoff Consulting + Solutions*

John Hurlock is the Director of Consulting Services for Sheshunoff Consulting + Solutions. John is responsible for the delivery of risk management business solutions to financial institutions. In this arena John is focused on financial risk management. He has over 25 years of experience in financial institutions. His first fifteen years were spent working for financial institutions of various size and complexity, and has spent the last eleven plus years in the business consulting arena. During John's banking career, he worked in several areas of banking including credit, treasury services and operations.

John has an undergraduate degree in Economics and an MBA from the University of Wisconsin. He is currently an adjunct professor for Webster University, teaching in their MBA program. He teaches Investment, Capital Markets and Management.