

Extending Your Enterprise



Enterprise Risk Management

Dushan Soza – MD WNS

September 19, 2008



The US subprime crisis

MAIN CREDIT LOSSES SO FAR

- * Citigroup: \$40.7bn
- * UBS: \$38bn
- * Merrill Lynch: \$31.7bn
- * HSBC: \$15.6bn
- * Bank of America: \$14.9bn
- * Morgan Stanley \$12.6bn
- * Royal Bank of Scotland: \$12bn
- * JP Morgan Chase: \$9.7bn
- * Washington Mutual: \$8.3bn
- * Deutsche Bank: \$7.5bn
- * Wachovia: \$7.3bn
- * Credit Agricole: \$6.6bn
- * Credit Suisse: \$6.3bn
- * Mizuho Financial \$5.5bn
- * Bear Stearns: \$3.2bn
- * Barclays: \$3.2bn
- * *Source: Bloomberg and company reports*

Key points to note

- As of May 2008, \$225 billion subprime related losses
- Subprime is also referred to as 'high risk' loans
- Subprime crisis caused due to rising interest rates, falling property values and other macro-economic factors
- However, the real reason can be attributed to poor underwriting process that was followed by the lending institutions and the lack of good governance practices by institutions that bought the subprime mortgages

Some key questions

- **What is mortgage underwriting?**
- Mortgage underwriting is the process a lender uses to determine if the risk of lending to a particular borrower is acceptable. Most of the risks that underwriters consider fall under credit, capacity and collateral. It is always up to the underwriter to make the decision on whether to approve or decline a loan.
- **So why are we facing the subprime crisis despite the underwriting processes that existed?**
- Although the institutions that lent money to prospective home owners had great underwriting processes and systems, the underwriter's decision was final, which could be against the system generated decision. In effect, lending institutions were following poor risk management practices. In addition, other factors such as the rising interest rates, falling property values and other macro economic factors contributed to the meltdown.

Some key questions

- So if the lending institutions flouted underwriting norms, why is the problem so widespread?
- The lending institutions passed on the subprime mortgages to other banks and investment funds in the guise of complex financial products. As a result, banks are now exposed to this bad debt.
- So are you saying that effective ERM processes could not have prevented the crisis?
- Of course yes. As part of Enterprise Risk Management (ERM), many financial institutions' quantitative risk models accurately illustrated the threat much before the subprime crisis caused a market meltdown. However, while the quantitative models did their job, the institution's management did not. ERM is only as good as the decisions that are taken by the entity's management. It's not the entity's ERM program, but management, that has primary responsibility for controlling risk.

Let's talk about ERM...

Local Going Global.....Are You Prepared?

In the past decade, with the surge in physical and telecom connectivity, a lot of companies have gone 'global'. Globalization is great, but do we understand the risks that it throws up....?

- Exposure to a different set of natural disasters
- Geo-political and socio-economic instability
- Foreign exchange fluctuation losses
- Lack of skilled manpower
- Lack of understanding of overseas regulation and legislation
-and many more

How can management prepare itself for identifying and mitigating risks in a globalized environment? Some questions that keep management awake are:

- How can we identify risks relevant to our business in a timely manner?
- How do we develop a 'risk adjusted' business strategy?
- How do we know whether we are over / under exposed to risk?

Solution.....Enterprise Risk Management

What is it? Simply put.....

“It is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” - COSO

Key points to note though

- Enterprise Risk Management (ERM) is not an end in itself, it is a means to achieve the end – meeting organizational objectives
- To succeed, ERM needs active support from the Board and senior management
- ERM needs to be integrated into the strategy setting phase – a strategy that is not ‘risk adjusted’ is most likely going to be misaligned with the organization’s risk appetite
- Unlike traditional risk management, ERM lets management focus on both, risks and opportunities

Why ERM?

Because ERM helps management:

- Define objectives – Carrying out risk management activities without definition of an organization's objectives is akin to a soldier in a war without a mission. If the organization plans to grow aggressively in new verticals (this would be a strategic objective), their risk management strategy would vastly differ from an organization that plans to grow at a modest pace. Without the definition of objectives, the risk management strategy may be completely misaligned.
- Define its risk appetite and develop a risk adjusted strategy – It is surprising but most organizations have not defined their risk appetite. Defining risk appetite is critical as it helps management strategize and take decisions that are within the organization's risk boundaries.
- Focus only on events that affect the achievement of organization's objectives – There are numerous events that occur across the globe. However, not all events impact the achievement of an organization's objectives. ERM assists management in addressing only those risks that impact the achievement of the organization's objectives.

Why ERM?.....Contd

Because ERM helps management:

- In reducing operational surprises and losses – ERM is not designed to be a crystal ball gazing exercise. However, ERM forces management to consider risk factors not only at the time of strategy setting but even while taking day-to-day operational decisions (risk tolerance). This reduces the uncertainty factor and creates a better managed company.
- Identify opportunities – ERM is different from traditional risk management, in that it requires management to identify ‘events’ and not just risks that affect the achievement of objectives. Events can be both risk and opportunities.

Eg, Take the outsourcing industry; if the price of crude increases to USD 200 per barrel, there could be a slowdown in business outsourced by the transportation industry; however, this would give rise to opportunities of providing more high-end consulting services on better resource utilization or could give rise to new services supporting tele-workers.

COSO ERM Framework¹



- 4 categories of objectives – demonstrates what management would like to achieve starting at the strategic level
- 8 components – provides the flow of activities for rolling out ERM within the organization thereby achieving organizational objectives
- Organizational divisions – demonstrates that for ERM to be effective, all units within an organization need to be engaged

1. Enterprise Risk Management – Integrated Framework and Enterprise Risk Management – Application Techniques – COSO, September 2004

Suggested ERM Rollout Approach

Tone at the top – It is important that leaders are convinced and believe in the benefits of implementing ERM. Visible and tangible support from the Board and CXO level executives is a must.

Risk management organization structure – Define an organization structure that lays down the roles and responsibilities (KPIs) clearly for the Board, the Risk / Audit Committee, the CEO, the CRO and BU owners.

Risk management philosophy – Draw up a risk management philosophy that lays the vision of risk management for the organization and serves as a ‘guide’ for employees. This should be circulated to, read and practiced by all employees. Risk management should be everyone’s responsibility.

Strategic Objectives – Strategic objectives (derived from the organization’s mission and goals) should be documented clearly. This is essential as strategic objectives will drive the formulation of strategies and related objectives – operational, reporting and compliance.

Suggested ERM Rollout Approach... .Contd

Define Risk Appetite – This is one of the most difficult but interesting tasks. Conduct a workshop for all C’X’O level personnel to arrive at the organization’s risk appetite. There are various ways to arrive at risk appetite. One of the ways to represent risk appetite is to prepare a matrix with the risk category on one axis and the appetite category on the other.

<i>Risk Category</i>	<i>Risk Appetite</i>	Averse	Minimal	Cautious	Open	Hungry
Financial						
- Inability to meet committed financial targets		X				
- Impact on Profitability				X		
Reputational						
- Loss of customer-confidence		X				
- Loss of employee-confidence				X		
- Loss of supplier-confidence				X		
- Loss of investor-confidence				X		
- Decrease in credit rating				X		
Operational / Internal Processes						
- Deviation from internal policy and processes			X			
- Impact on operating capability			X			
- Violation of code of ethics		X				

Since risk appetite is a relative term, defining it in absolute terms may not be possible. Eg, it is difficult to answer the question – “Provide a value commensurate with your risk appetite.” as opposed to “What risk are you willing to accept for an investment that could fetch 30% ROI?”

Suggested ERM Rollout Approach.....Contd

Related Objectives (Pilot Project) – Define related objectives (for only one business unit / function initially) keeping in mind that these are in line with the strategic objectives. Also, this will ensure identification of only those events that affect the achievement of organizational objectives.

Define Risk Tolerances (Pilot Project) – Define risk tolerances for each of the related objectives keeping in mind that the tolerance levels do not violate the risk boundaries of the organization. Define monitoring measures to identify compliance with risk tolerance levels.

Event Identification (Pilot Project) – Identify events that are likely to affect the achievement of the related objectives (for the said BU / function). It is critical to identify a comprehensive set of events as some of these may be opportunities.

Suggested ERM Rollout Approach.....Contd

Risk Assessment and Response (Pilot Project) – For all events that pose risks to the organization, ascertain the likelihood of the risks materializing and prepare an appropriate response plan. All opportunities identified should be rolled back into the strategy review process.

Enterprise-wide roll out – Once management identifies benefits of implementing ERM in the pilot environment, roll out ERM across the enterprise. The benefits will be huge as what could appear to be a risk for one vertical (Transportation) could be an opportunity for the other (Analytics).

Roles and Responsibilities



Case Study

Our BCP approach and how it ties in to COSO ERM

Our BCP Approach

- Business Impact Analysis (BIA) – Identify critical business processes, the permissible level of degradation and the recovery time objective
- Risk Assessment – Conduct a risk assessment to identify what events that could affect the continuity of business operations
- Business Continuity Strategy – Prepare a strategy that covers the people, infrastructure and process components to recover critical business processes

How it ties in to COSO ERM

- Developing the BIA helps the business identify its objectives – what it wants to recover and how soon. This also helps in defining the risk appetite – how much degradation is acceptable to the business?
- Conducting a risk assessment helps us focus only on those events that are likely to present a business disruption scenario. This also helps us focus on investing in only those countermeasures that would promote business continuity while developing our risk response strategies

Our BCP approach and how it ties in to COSO ERM

Our BCP Approach

- Business Continuity Plan / IT Disaster Recovery Plan – Develop a detailed plan that lays down the steps that would be undertaken to recover critical business processes
- Testing and Training – Test the plan regularly to establish it's operating effectiveness and train individuals for performing their tasks effectively

How it ties in to COSO ERM

- Development of the BC and IT DR plan itself draws on the COSO ERM component of risk response that lays down the activities that would be carried out to restore business operations
- Testing the BC plan through a series of scenario / work area recovery tests is equivalent to monitoring the process of identification of risks and validity of risk responses

What this approach has got us through

- The maximum amount of rain in an urban area anywhere in the world – Mumbai in July 2005 (~2,500 FTE affected)
- Serial bomb blasts in suburban trains in Mumbai that paralyzed the city's road and rail traffic infrastructure in July 2006 (~ 3,500 FTE affected)
- Multiple bomb threats at our Pune center in July 2006 (~ 950 FTE affected)
- Very heavy rains in Mumbai in August 2006 over a period of 3 days that paralyzed city traffic once again (~ 3,500 FTE affected)
- Riots in Maharashtra in November 2006 over a period of 2 days that affected all cities where our operating centers are located – Mumbai, Pune and Nashik (~ 9,000 FTE affected)
- Sri Lanka – Curfews , Elections , Independence day, SARCC, strikes, Petrol shortages, bombs / threats , road blocks , staff & expat treatment

Thank You