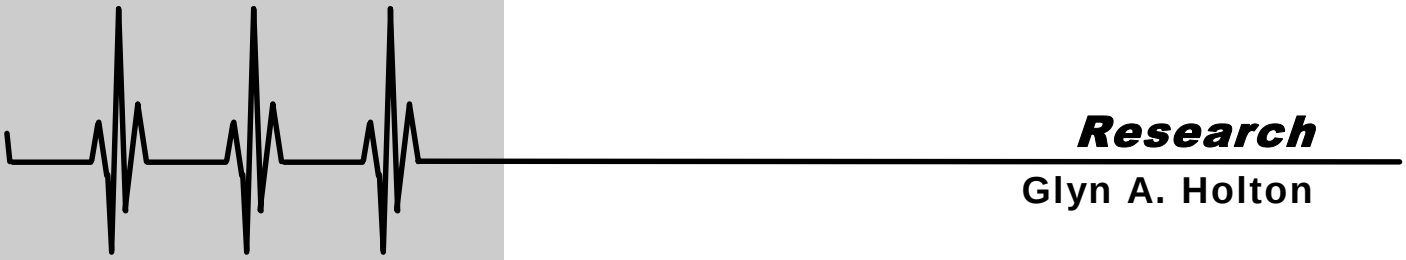
Enterprise Risk Management



Research

Glyn A. Holton

In case the music stops . . .

Enterprise Risk Management

Contents

Contingency Analysis

Post Office Box 961
Boston, MA 02199-0961
(617) 536-7434

This document can be accessed on-line at:
http://www.contingencyanalysis.com/_frame/frameerm.htm

Enterprise Risk Management

1. Introduction

All organizations are in the business of placing capital at risk in pursuit of ventures which are uncertain. This includes financial institutions, governmental bodies, corporations and non-profit organizations. They all have goals, and they allocate resources to pursue them. Because all organizations face uncertainty in achieving their goals, they all face risk.

Enterprise risk management is about optimizing the process with which risks are taken. It has become a critical issue for the 1990's because organizations have started suffering spectacular losses—often from risks they never should have taken in the first place. Examples include:

- **Orange County (November 1994):** Orange County's Investment Pool lost $1.7 billion from structured notes and leveraged repo positions. The treasurer, Robert Citron, took the positions with oversight from the county's five-person board of supervisors. The riskiness of the pool's investments was publicly discussed when Citron ran for, and won, reelection in 1994. Members of the board of supervisors claim that they did not receive critical information which would have indicated the risks that Citron was taking.

- **Barings Bank (February 1995):** Barings Plc lost $1.5 billion because a Singapore-based trader, Nick Leeson, took unauthorized futures and options positions linked to the Nikkei 225 and Japanese government bonds (JGBs). At the height of his activities, Leeson controlled 49% of open interest in the Nikkei 225 March 95 contract. Despite having to finance margin calls as the

bank lost money, the Barings' board and management claim to have been unaware of Leeson's activities.

- **Daiwa Bank (September 1995):** One of Daiwa Bank's US-based bond traders, Toshihide Iguchi, concealed $1.1 billion in bond losses over a ten year period. When management learned of the losses, they attempted to hide them from US regulators. Ultimately, Daiwa was forced to cease its US operations and was fined $340MM in a plea agreement with US prosecutors.

- **Sumitomo Corp. (June 1996):** Sumitomo's head copper trader, Yasuo Hamanaka, disguised losses totaling $1.8 billion over a ten year period. During that time, Hamanaka performed as much as $20 billion of unauthorized trades a year. He was able to hide his activities because he headed his section and had trade confirmations sent directly to himself, bypassing the back office.

In recent years, numerous organizations have suffered staggering losses such as these. These four, however, are some of the most significant. They illustrate two common characteristics. Each one:

- Was directly caused by the actions of a single individual.
- Could easily have been prevented through appropriate oversight.

Losses such as these never used to occur. In the past, companies might go bankrupt or suffer losses, but the forces that did them in were macroscopic—competition, mismanagement or adverse economic conditions would bleed a company's vitality. Today, an individual can pick up a phone and place billions of dollars in notional capital at risk. This is new.

The risk does not only come from derivative instruments. It arises from the many sources of leverage which are available today. These include derivatives, repos, securities lending and structured notes. Such tools have increased liquidity in the markets and enable institutions to efficiently manage many of their risk exposures. In the wrong hands, however, they can devastate an organization.

The problem is not the financial tools, but the people who use them. While many financial tools are new, the problem of people acting fraudulently, or just irresponsibly, has always existed. In the past, risks were unleveraged, so trading losses were limited. They might cost a few individuals their careers, but they would rarely make the newspapers. Today, people take the same types of risks, but they leverage them, and the losses burgeon.

Leverage doesn't only magnify market risk. As margins for error contract, other risks increase, including credit risk, liquidity risk, operations risk and legal risk. Organizations are focusing on all of these. Through enterprise risk management,

they seek comprehensive solutions—not because the problem is new, but because the consequences of failure have become enormous.

Regulators are also motivating a process of change. Awakened to the threat of leveraged risk, they are pursuing initiatives that:

- Enhance the disclosure of off-balance-sheet risks
- Promote corporate risk management
- Ensure that institutions are sufficiently capitalized for the risks that they take
- Reduce systemic risk

Finally, organizations are embracing enterprise risk management because it makes good business sense. Today, they actively make the decision to change the way they take risks. They implement innovative procedures. They install new technology. They actively reshape their corporate culture to facilitate better risk taking.

Implementing an effective strategy of enterprise risk management is not easy, and for each organization, it is different. There are, however, three fundamental elements which should comprise any risk management strategy:

- Corporate culture
- Procedures
- Technology

The importance of each of these will vary depending upon the needs of an organization. Each will, however, be important in some sense or another. For example, a university endowment which manages all its assets externally, may not need much risk management technology, but it will need to ensure that the investment managers it hires do have—and appropriately utilize—such technology.

These three elements of enterprise risk management are discussed in the following sections.

2. Culture

In the introduction, I identified four examples of institutions which suffered dramatic losses. While the immediate cause for each loss was adverse market moves, the fundamental problem was cultural. Each institution had a corporate culture which was incapable of confronting irresponsible behavior.

It is a fact that an organization will only manage risk if its members want to manage risk. Regulators struggle with this every day. They can force a bank to implement a multi-million dollar value at risk system. They can require an

insurance company to implement hundreds of pages of procedures. But they cannot force an institution to effectively manage risk.

It is individuals who decide whether or not they are going to manage organizational risk. Unfortunately, there is a big incentive for them to choose not to. The very sorts of behavior which reduce organizational risk entail significant personal risk. For example:

- A clerk who blows the whistle on a trader may get the problem resolved, or he may end up without a job.

- A board member who wishes to pursue risk management must stick her neck out. At the risk of appearing alarmist, she must suggest that potentially significant problems are not currently being addressed.

- A trader—whose compensation depends primarily upon his reputation in the organization—can only manage risk if he first acknowledges that he is capable of making mistakes.

- An executive who wishes to address the risk of employee fraud may risk alienating his own colleagues.

Risk management is about rocking the boat, asking questions and challenging the establishment. No one can manage risk if they are not prepared to take risk.

While individual initiative is critical, it is corporate culture which facilitates the process. Corporate culture defines what behavior the members of an organization will condone, and what behavior they will shun. Corporate culture plays a critical role in risk management because it defines the risks which an individual must personally take if they are going to help managing organizational risks.

A positive risk culture is one which promotes individual responsibility and is supportive of risk taking. Characteristics include:

- **Individuals making decisions:** Group decision making is bad risk management because no one is accountable. When a single person makes a decision—possibly with the help or approval of others—that individual is personally accountable. His reputation is on the line, so he will carefully analyze the issues before proposing a course of action.

- **Questioning:** In a positive risk culture, people question everything. Not only does this identify better ways to do things. It also ensures that people understand and appreciate procedures.

- **Admissions of ignorance:** Mark Twain once said "I was gratified to be able to answer promptly. I said I don't know." Admitting that we don't know

entails significant personal risk. A positive risk culture supports such honesty at every level of an organization.

No risk culture is perfect. Fortunately, few are beyond repair. The challenge of enterprise risk management is to honestly assess an organization's culture, and then work to improve it.

3. Procedures

When you mention procedures, people are likely to roll their eyes as thoughts of red tape and bureaucracy flood their thoughts. This is unfortunate. Used correctly, procedures are a powerful tool of enterprise risk management.

The purpose of procedures is to empower people. They specify how people can accomplish what needs to be done. It is only when procedures are neglected or abused that they become an impediment.

The success of procedures depends critically upon a positive risk culture. Hundreds of pages of procedures, neatly typed and sitting on a shelf, are useless if no one uses them. However, even a simple set of procedures can make an enormous difference for an organization if people believe in them and take personal responsibility for upholding them.

Procedures systematize the process of risk management. Consider market risk limits. These are a form of procedure which systematize oversight of trading risk. They make explicit how much risk is too much risk for any given segment of a portfolio.

Without risk limits, someone would have to track the risks being taken by individual traders and apply their own subjective judgment as to how much is too much. Should they decide to act on their subjective judgment that a trader is taking too much risk, the affected trader may reasonably feel that the decision is arbitrary or unfair—she might ask: "what about the market opportunity I was pursuing or the client whose needs I was trying to meet?"

Whenever procedures do not exist, there is increased potential for disagreement, misunderstanding and conflict. A lack of procedures increases the personal risk that individuals must take if they are going to manage organizational risk. Accordingly, a lack of procedures tends to promote inaction.

Effective procedures, on the other hand, empower people. They lay out specifically what people should do—and what they should not do—in a given situation. By reducing uncertainty—individual risk—they promote action.

Examples of procedures include:

- Board procedures: Every board of directors or governing body should operate under a set of procedures which address conflicts of interest, clarify personal responsibility and facilitate the discussion and resolution of difficult or contentious issues.

- Lines of reporting: Everyone in an organization should report to a single person. The line of reporting should be explicit. A worthwhile illustration for this is the Bank of England's report on the Barings collapse. That report identifies four different people who may have had oversight responsibility for Nick Leeson.

- Trading authority: Whenever an organization engages in a new form of market activity—such as the use of a new form of transaction, a new hedging strategy or proprietary trading—there should first be a formal review and approval process. A streamlined procedure should apply for granting new responsibility to any trader.

- Risk limits: Market and credit risk limits represent procedures for managing risk. There should also be procedures for establishing and reviewing such limits in order to assure that the system of limits remains effective.

Also, every organization should have procedures for changing procedures. Because procedures become outdated over time, it is easy for organizations to change how they operate without formally recognizing that the change is taking place. Informal practices evolve out of habit, instead of a deliberate process. Because they may be adopted out of necessity or convenience—without considering how they impact organizational risk—they, too, are a source of risk.

Often, periods of change are a time of increased risk for an organization. Procedures for changing procedures are an excellent mechanism that encourage people to recognize changes as they are taking place and formally address the risks that they pose.

Most organizations first develop procedures for regulatory purposes. Their regulators require them to implement certain procedures, and so they do. As regulators are well aware, this can be a two-edged sword.

1. On the positive side, when a regulator requires certain procedures, those procedures are typically sound tools for reducing risk.

2. On the negative side, regulatory procedures are primarily intended to minimize risk, which is different from optimizing risk. Their main purpose is to protect third parties or to control systemic risk.

Every organization should supplement regulatory procedures with their own procedures which embrace a process of risk optimization. Indeed, the more proactive an organization is in developing its own procedures, the more effective that organization will be at enterprise risk management.

Through such a process, an organization will not only implement procedures which are in tune with its goals, it will also be implementing procedures for the right reason. A useful analogy for this is drivers stopping their cars whenever they come to a red light. They may do so because they fear being caught running a red light. A better situation, however, is if they stop out of concern for their own safety. The best procedures are those which an organization wants to implement and promote.

4. Technology In Perspective

For many institutions, such as banks, investment management firms or insurance companies, technology will be a critical component of any risk management initiative. For other organizations, especially those which do not manage assets internally, technology is less important.

For institutions which rely heavily on technology, there is always a risk of the cart being placed before the horse, and technology becoming the focus of risk management. If an organization launches a risk management initiatives by first allocating money to the project and then issuing an RFP, that can be a warning sign.

A more staged approach starts off by recognizing that risk management is primarily about people—how they think and how they interact with one another. Technology is just a tool. In the wrong hands, it is worse than useless, but applied appropriately, it can transform an organization.

A good approach to implementing an enterprise risk management initiative is:

1. Initially allocate minimal funding for the initiative, but ensure that board members, senior management or other supervisors are involved in the process.

2. Start by planning a risk management strategy that involves no technology at all. This can be an empowering exercise. It focuses participants on the procedural and cultural issues of risk management. Ultimately, it is these which determine the success of an initiative.

3. Once you have decided on a strategy for managing risk, then determine where technology needs to be incorporated or where it can enhance the strategy.

The next few sections outline the important role that technology can play in enterprise risk management. The focus of the discussion is on technology within a trading environment because that is where the greatest technology demands exist. Because readers are probably familiar with technologies such as databases, distributed systems and object oriented programming, the discussion does not focus on the "how" of technology so much as the "why." The goal is to illustrate the ways that technology can impact how people work and interact with one another. Technology can reshape corporate cultures and facilitate innovative procedures. Here is how…

5. Data Aggregation

Information is essential to enterprise risk management. However, before it can be processed, analyzed or acted upon, it must first be made available to the systems and individuals who need it.

In the introduction, I gave four examples of institutional losses: Orange County, Barings Brothers, Daiwa Bank and Sumitomo. Each could have been prevented if decision makers had the right information. Three of those cases, involved the fraudulent falsification of information.

Accordingly, institutions should manage their information flows with the assumption that individuals will attempt to corrupt or undermine the process. Automation can play a valuable role by eliminating opportunities for manual intervention in such processes as deal capture, confirmations, reporting and funds transfers. This, however, is just one benefit of automated data management.

Even without fraud or human error, data management has always been a bottleneck for enterprise risk management. Managing such risks as an organization's total yield curve exposure, or its total credit exposure to a counterparty is impossible without comprehensive information about those exposures.

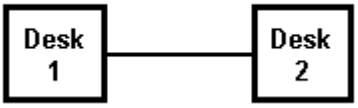
For example, within a typical trading operation, yield curve exposures will arise from the activities of almost every desk. Some of those exposures will be intentional—the Eurodollar desk may take outright positions. Others will be consequential to a desks' primary responsibilities—the foreign exchange desk may generate yield curve exposures by hedging forward positions with spot trades.

Credit exposure poses a similar problem. Exposures to a single counterparty can arise throughout an institution. Lending, underwriting, the derivatives desk, the foreign exchange desk—almost every functional unit may create exposures to a counterparty. Those exposures can be highly varied and complex—short-term, long-term, settlement, pre-settlement, stochastic, etc.

Before an organization can attempt to manage risk on an enterprise-wide basis, it first must collect and communicate all necessary information relating to those risks. In the past, organizations have had limited ability to do this. They have faced too many different and complex risks—and professionals have had no convenient means of communicating exposures across an organization.

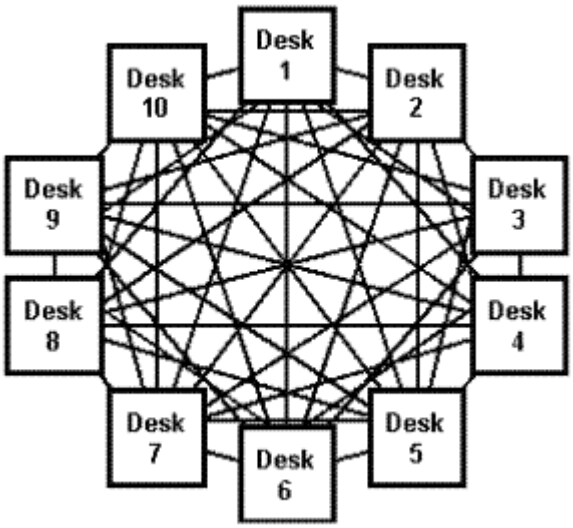
Consider the simple case of a bank which has just two trading desks. For these desks to cooperate in managing risks, there would need to be just one line of communication.

Two Desks, One Line of Communication
Exhibit 1



Suppose, however, that the bank had, not two desks, but ten. In this case, the lines of communication would grow from one to as many as forty-five. Trying to manage risk across these forty-five lines would become a monumental task. For traders, communicating with other desks could become a full time job. Add to this the differing conventions that might exist on each desk, the need to coordinate desks in multiple time zones, and the task of also communicating with the back office, credit department, sales and risk management—the problem becomes insurmountable.

Ten Desks, Forty-Five Lines of Communication
Exhibit 2



In the past, this problem prevented organizations from managing risk on an enterprise-wide basis. Instead, each desk or each department would be given broad authority to manage those risks which arose from its own operations. Instead of having each professional manage the specific risks for which he or she was best qualified, individuals were called upon to be generalists. Each would

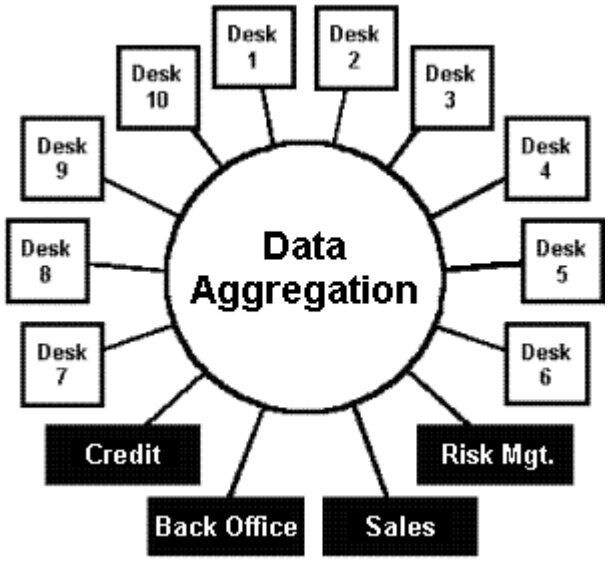
manage multiple risks. In this environment, each desk would be given its own credit risk limit for each counterparty and its own market risk trading limits.

Today, technology makes it possible to effectively communicate information—across desks, across departments, around the globe and in real time. That technology solution is data aggregation.

As the trading environment becomes automated, information can be automatically captured as it is generated—both streamlining the process and avoiding errors or fraud. As data is captured, it can be posted to a central data repository. From there, it can be accessed by all systems, all desks and all departments that need it.

This solves the communication problem. The need for human intervention—phone calls, memos, meetings—is eliminated. As information is generated, it is automatically posted. When another desk or department needs that information, it is automatically retrieved. Each desk and each department needs just one line of communication—one with the data repository.

Data Aggregation Facilitates Communication
Exhibit 3



Data aggregation is not a new concept. Corporations have been trying to aggregate data since the time when they installed the first mainframe computers. Today, however, it is an achievable goal enterprise wide.

6. Risk Analysis

"How much risk are we taking?" The question is so simple—and yet profound. In one form or another, it underlies enterprise risk management. In the past, organizations would look to their profit & loss statement to answer the question. Volatile profits meant high risk. You couldn't argue with that.

A problem, however, is that profit & loss is a retrospective measure of risk. We all know that Barings Bank was taking a lot of risk in February of 1995. That brutally accurate fact, however, arrived too late to avoid catastrophe.

Indeed, for many risks, the profit & loss statement may reveal little or no information—even retrospectively. A credit loss might impact profit & loss years after an exposure is first taken. The profit & loss statement may provide no indication whatsoever of liquidity risk. That risk tends to strike infrequently, but with devastating effect. The first time a liquidity crisis impacts the profit & loss statement is often the last.

In order to manage risks, organizations need to be able to measure those risks prospectively. They need to know, based on their positions today, how much risk they are actually taking. This is a difficult question to answer.

Data aggregation does not solve this problem. It brings all the necessary data together, but a list of contracts or a catalog of counterparties can not tell you where your risks lie. Somehow, that wealth of data must be processed and converted into a measure of risk.

Organizations are addressing this challenge with statistical risk measures. For market risk, they are using value at risk (VAR). For credit exposure, they are using expected exposure or maximum exposure. Such risk measures are powerful because they can summarize a complex risk with a single number.

For example, value at risk incorporates all of a portfolio's holdings as well as the volatilities and correlations of applicable risk factors. It then synthesizes this wealth of information to produce a single number. That number represents the upper bound on a confidence interval for how much money the portfolio could lose over a specified horizon.

Because value at risk is based on a portfolio's current holdings, it is a prospective measure of risk. It tells you how much risk you are taking now—not how much risk you were taking last week or a month ago. Furthermore, because it takes into account market volatilities and correlations, it captures all hedging and diversification effects.

Statistical measures for credit exposure are similar. Based upon the existing portfolio of contracts with a counterparty, they summarize the potential credit exposure, taking into account all market volatilities and correlations.

A shortcoming of statistical risk measures is the fact that they can be extremely computer intensive. In many circumstances, they can only be calculated using Monte Carlo simulations. Indeed, when such simulations are applied to large portfolios containing thousands of positions, they can take hours to perform.

For this reason, institutions are turning to ever more powerful computer systems to support their risk analysis. Distributed systems which parallelise a simulation and run it simultaneously on multiple computers offer much potential. When these are used in combination with the latest simulation techniques, many sophisticated forms of statistical risk analysis can be performed in real time or near-real time.

7. Automated Oversight

With statistical risk measures, and the ability to assign a precise number to risks, oversight can be automated. The process starts by assigning each department, each desk and each trader explicit authority to take specific risks. This authority is articulated as risk limits.

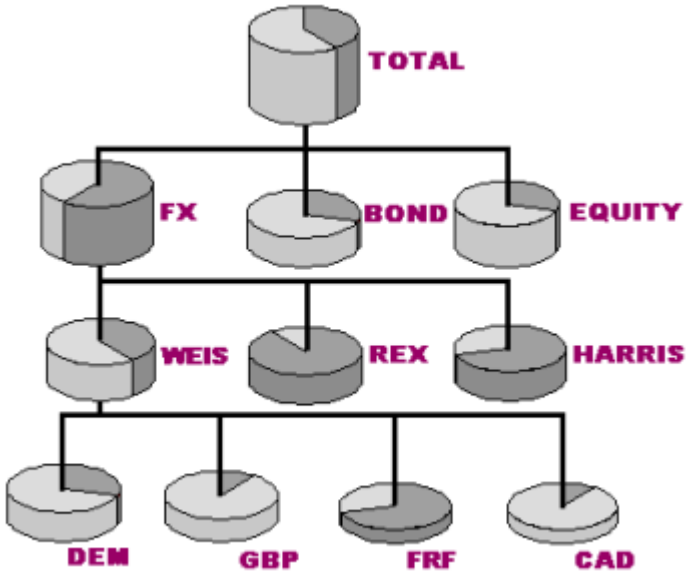
For example, a foreign exchange trader who trades three different currencies might be given a risk limit for each currency. Those limits would be expressed in terms of value at risk. The risk management system would track the trader's value at risk arising from exposure to each of the currencies to ensure that they remained below the respective limits. The trader would also have a total value at risk limit. This would cap the total risk he was allowed to take, irrespective of source.

In addition to trader-specific limits, there would be overall limits for each desk and total limits for the entire trading operation.

Because a system of limits can become quite involved, it is worth visualizing the process. Exhibit 4 illustrates a cross section of a hypothetical trading operation's market risk limits.

In Exhibit 4, each risk limit is depicted with a cylinder. The height of each cylinder corresponds to the size of the limit. For example, the limit at the top, which covers the total risk of the entire trading operation, is quite tall. The per-currency limits for an individual trader at the bottom of the exhibit are much shorter.

Example: Limit Structure
Exhibit 4



The extent to which each cylinder is shaded orange corresponds to the utilization of that limit. For example, if a cylinder corresponds to a $2MM limit, and the value at risk under that limit is $1.2MM, the cylinder would be 60% shaded.

In Exhibit 4, the trading operation has three different trading desks, covering foreign exchange, bonds and equities. The foreign exchange desk is utilizing over 50% of its limit. In the exhibit, its sub-limits are shown, showing limits for three traders. Of these, trader Rex is close to hitting his limit. Trader Weis's per currency sub-limits are shown. Weis has significant exposure to the French franc, but less exposure to other currencies.

When a limit structure such as the one in Exhibit 4 is supported by risk measurement technology which can precisely measure utilization under each limit, trading risk oversight becomes automated. If a trader exceeds a limit, it is immediately caught. The system then informs the risk management unit, appropriate managers, the trader and the trader's colleagues on the trading floor. In this way, a clear standard is set for appropriate behavior, and everyone knows if someone violates the standard. The system becomes self-policing because everything happens out in the open.

8. Conclusion

A clear distinction should be made between risk management and risk taking. Risk management oversees and ensures the integrity of the process with which

risks are taken. To maintain objectivity, risk management cannot be a part of the risk taking process. Individuals who manage risk need to be completely independent from individuals who are responsible for taking risk.

Enterprise risk management is a complex and multifaceted process which varies from one organization to the next. It should be viewed as an ongoing process which needs continual oversight, planning and modification as needs evolve.