EMERGING ISSUES IN RISK AND SOUND RISK MANAGEMENT

By
Buwanekabahu Perera

Born of financial deregulation, nurtured by globalization, disturbed by global terrorism with deteriorated human values and business ethics, rise in business sophistication confirmed by the arrival of the internet, "change" has been a recurrent theme in business literature in the past two decades, and the "change" appears to be the only "constant" for the future. The transformations brought by these forces have created entirely new risks that financial institutions are only beginning to address. Subtler changes, such as widespread public intolerance of corporate interest and the increased importance of corporate reputation, demand a sophisticated awareness of social and legal issues.

In this changing world, some of the emerging issues in relation to Risk Management are

- e-Commerce.
- Brands and reputation.
- Human psychology and financial crime.
- Environmental risk and extreme events linked to natural disasters.
- Shareholder expectations and Enterprise-wide Risk Management.[ERM]
- Complexity of Operational Risk
- Global Terrorism and Political risk
- Systemic Risk and Financial (de) Regulations. [Basel II]
- And many more-rapid advancement in science & technology i.e GM Food items and Global Warming

Hence the scope of discussion on "Emerging Issues in Risks" is very wide, but in this article it is confined to two areas, namely

1. Brands and reputation – titled as "Branding and Reputational Management"
2. Shareholder expectations and Enterprise-wide Risk Management.[ERM] , titled as – "Philosophies of risk, shareholder value, the CEO and the Board"

The final section of this article is focused on the basic tools of Risk Management, titled – **"A common sense approach to enterprise-wide Risk Management"**

Branding and Reputational Management

How much is strong branding of financial products is capitalised in Sri Lanka and to what extent do financial institutions protect these brand values from "copy cats" and poachers in this competitive market place ?

Brands are now lifestyle appendages. In such a world, those who own them had better protect them. Companies i.e Financial Institutions are now urged to manage customer/brand relationships and experiences actively. Protection involves defending business reputation to customers, depositors, suppliers, trade partners, and employees. In addition, brands are a promising target for consumer advocates. Through exchanges on the internet, they can quickly tackle such issues as brand ingredients, company history, environmental attitudes and behavior, work and economic policy, and so on. Furthermore, the internet has empowered consumers as never before. Therefore the best practice in reputation management requires considerable reflection and honesty. Virtually anything an enterprise does or says will either enhance or destroy brand value. Reputation management has become a natural extension of brand care — good reputations sell products and services, poorly managed ones destroy shareholder value. Hence Branding puts a high value on reputation management Companies i.e Financial Institutions, need to treat reputation risk in the same way as they treat risks to other corporate assets. They should define the risks to reputation, prioritize them, and establish strategies to protect the reputation of the organisation if they want to avoid a crisis of confidence among stakeholders and the wider public i.e customer / depositors. Though decisionmaking responsibility for reputation issues resides with the CEO, this task should be carried out by a company-wide team. In particular, these strategies should capitalize on emerging technologies and the networking power of the Internet.

In an environment in which functional differences between products and services, especially in the financial services sector, have been narrowed to the point of near invisibility by the adoption of Total Quality Management, brands provide the basis for establishing meaningful difference between competitors.

Competitiveness now depends on being able to satisfy not just the functional requirements of customers, but also their intangible needs. It means understanding, not just what you can "do" for them, but also what you can "mean' to them. There is now wide spread acceptance that brands play an important role in generating and sustaining the financial performance of branded business, which is now extending towards the Financial Service Sector. With high level of excess capacity in the Financial Service Sector i.e Banking Industry, strong brands would no doubt help these institutions to communicate why their products and services are uniquely able to satisfy customer needs.

But having a strong brand alone is not sufficient, one needs to protect it from "copy cats" and poachers in this competitive market place. Brand protection is often viewed as a legal issue. Names or marks that function to identify a product are used as trademarks to protect the brand. In many countries, trademark and copyright law governs this protection. Legal brand protection creates a monopoly, which is usually unlimited in time as long as the product is sold. Trademark law

prohibits another company from using the same or similar names, logos, or marks if these brand identity elements are already in use and if such use would be likely to cause confusion in the marketplace. Legal brand protection is thus an attractive way of securing long-term competitive advantage.

A brand is, of course, much more than a name and a logo. Today's brand strategists say brands evoke distinct associations; they ascribe human personality traits to brands; they speak of "long-term" relationships with customers, rather than 'transactional exchanges'. Brands carry emotional attachments. In short, brands have the potential to provide customers with a variety of pleasant, or unpleasant, experiences.

Given this new complex understanding of the brand, its protection now has to extend far beyond the legal arena. Brand experiences can be damaged by "copycats" or counterfeiters. Simply protecting brands from aggressive competitors is no longer sufficient.

Instead, financial institutions must actively manage the 'brand—customer relationship." Brand protection extends to the entire organisation. It has become a matter of managing the organisation's reputation in the eyes of its various stakeholders - including its customers, depositors, trade partners, and employees.

Anything a company does or says can add to — or destroy — brand value. However, all companies are increasingly held accountable and responsible for an assortment of actions by a variety of stakeholder groups. Consumer activism is not limited to advertising messages. More and more, consumers are interested in anything related to the brand: the ingredients of its products; the company's history; the company's attitude and behavior toward environmental issues; its work policy; and its stance on a range of other economic, social, and political issues. Today's companies and their brands are being scrutinized as never before.

Reputation management is thus a natural extension of brand management. Done well, reputation management can bring considerable benefit to a company. A decent reputation helps to sell products and services, recruit new talent and attract new customers. Done poorly, it destroys shareholder value. A bad reputation is an obstacle in selling to outlets and consumers, and in recruiting new talent. Reputation management also plays a role in such tactical decisions as recruitment of the right people. A company's human face, especially in a financial institution, can make all the difference in the world to corporate reputation.

Since branding could apply to the entire organization, everybody in the organization has a role to play in reputation management. To represent the brand in the right way, all employees need to know the brand and live with it. In a wide variety of situations and in day to day operations – for example when meeting customers, communicating to the public, and industry gatherings and conferences, - the bank employees are representing the corporate brand, and should thus be prepared to engage in behavior that is consistent with it.

Brand reputation management - In order to practise effective reputation management, one needs to consider four interrelated aspects.

First - Reputation management must be broadly conceived. Because almost anything may be viewed as a brand, all companies in all industries must consider reputation management. Over the

last decade, the concept of branding has been gradually broadened from its origins in the consumer packaged goods industry into many other forms of commercial — and even non-commercial — offers. Furthermore, reputation management is relevant for both old and new brands. —older-established brands will be held to the same standards as newer, trendy ones.

Second - Modern corporations consider brands as intangible assets. Thus, reputation management must be viewed as a way the Long Term Value of the brand [LTV]. In many cases, the intangible value of brands exceeds the value of a corporation's tangible assets. "Interbrand", the New York-based brand valuation consultancy, has estimated the value of the Coca-Cola brand to be more than 95 percent of all its corporate assets.

Third - Branding techniques can be found throughout the organisation. Of course, products are branded, but so are the promotional campaigns related to these products, and so in fact is the organisation as a whole. Indeed, many companies i.e financial institutions, that have traditionally focused on the branding of their individual products have discovered the corporate brand as an essential new marketing initiative.

It follows that reputation management cannot be delegated to any single department or function. Inside the organization, reputation management involves marketing, communications, public relations, various information technology functions, and even the chairman's office. Outside, it involves corporate identity companies, PR operations, and advertising agencies.

The often-neglected "human interface" between the bank and its customers can be enough to undo the best internal efforts at reputation management. It is critical to implement a unified reputation approach that covers all these aspects. Branding succeeds if it is coherent and consistent; the same applies to reputation management.

Fourth - Markets become real-time exchanges and conversations among consumers on the internet. Brand information — in all different forms and media — is available instantly and globally on the web. The internet empowers consumers, allowing them to post their views about a brand to a worldwide audience. Companies need to be able to deal with this new form of brand scrutiny, protect their brands, and manage their reputation online. This requires effective management of the corporate website and links to other sites; selective presence on other websites; fast and adequate response to electronic inquiries.

Reputation management is important in protecting the long-term value of a brand. It is not a cosmetic image management device, nor is it a mere strategy to sell more products. Reputation management speaks to the very heart of an organization. Just as it is difficult for an individual to put on a false face without being found out, so it is difficult for a company to espouse values that its actions do not support. On the web, it is easy to find out about a company's true nature.

From an ethical perspective, reputation management, thus, requires a consideration of values and competencies that are shared throughout the organization, and is best practised with reflection and honesty.

Corporate reputation is worth a great deal. Research carried out in late 1990's by Citibank and branding consultancy "Interbrand" showed that the total value of the FTSE 100 companies was

£824bn, of which tangible assets accounted for £240bn and goodwill accounted for £584bn. In other words, goodwill — of which reputation is a large part — accounted for 71 percent of total value. Ten years earlier, goodwill accounted for 44 percent of total value.

A recent article in Fortune stated: "[As] America's 10 most admired companies .... stand above the rest of corporate America in reputation, so do they tower over it in performance ... A 10-year investment [in them] would have yielded nearly triple the shareholder return of S&P 500 stocks." Reputation is now so important that the Turnbull report, which forms part of the UK's corporate governance guidelines, advises companies to treat it in the same way as all other assets. A survey carried out in December 2002 among risk managers in UK companies found that reputation risk was the greatest risk facing their organizations.

Reputation risk can be defined as the set of threats that affects the long-term trust placed in the organization by its stakeholders, which includes its customers, depositors, suppliers, staff, and shareholders. It covers risks to products, the company or the whole industry.

During a reputational crisis, to a specific product, company or in an industry, the senior managers of the relevant organizations would have experienced the classic symptoms in a crisis situation:

- a lack of information;
- growing consumer mistrust;
- increased attention from the press and media;
- loss of confidence among stakeholders;
- commercial and/or political pressure to respond
- internal conflict over what should be done to resolve the situation.

The characteristics of successful crisis management include:

- demonstration of decisive remedial action;
- access to the right information;
- high speed in communications;
- a consistent corporate message;
- a full appreciation of the needs of all stakeholders
- the ability to admit to mistakes
- a clear recovery strategy.

These characteristics are normally the result of good procedures, comprehensive planning, appropriate training and good early detection systems, all of which contribute to a reputation protection strategy. So how does a company establish such a strategy?

Protecting reputation

Responsibility for corporate reputation has typically resided with the CEO or the corporate communications department, whereas traditionally conceived risks such as exchange-rate risk or insurance have been the domain of the risk manager or finance department. Reputation risk falls between the two, cutting across many aspects of the business. It requires a small, cross-functional team to create and implement a protection strategy. This would typically from corporate communications, customer relations, the health and safety department, investor relations, the legal department, operations, public affairs, and risk management, with input from the chief executive or chairman. In setting up a program, they should conduct the following exercises.

Assessing the threats - The organization needs to have a clear understanding of the main threats to its reputation. These might manifest themselves through sustained media coverage, rapid falls in share price and loss of customer / depositor confidence. They can be caused by factors such as the reputation or the lack of confidence of the Board of Directors, high staff turnover destroying customer relationships, high degree of transactional errors, unethical trading and business practices, marketing failures, frequent system failures or more traditional risks such as product failure. This process of listing reputational risks requires honesty and doggedness.

Prioritizing reputation risks - Once the risks have been identified, they need to be prioritized in order to help managers determine where to devote effort and resources. This prioritization process should be linked to the organization's exist ing risk management strategies. The task force might evaluate the reputation risks according to their likelihood and their impact in order to establish a reputation risk ranking. For instance, an organization might feel that the likelihood of an earthquake on a key operation might be relatively low, but if it were to happen such an event would be catastrophic - the risk is therefore defined as small but significant.

Managing reputation risks - Examining reputation risks for their likelihood and impact only shows one side of the coin. The other side requires an assessment of the organization's ability to avoid the risk or respond to it, if it occurs. Once procedures for managing those risks have been identified, it is possible to map the reputation risks and analyze the gaps.

Monitoring reputation risks - Having mapped important risks, the organization should establish procedures to monitor early warning signs of them occurring or increasing. One of the important listening posts in an organization is the customer services department. This department will often be able to establish early signals of a trend occurring before the issue spills over into the public domain.

Responding to reputation risks - No organization will be able to avoid or preempt all of the risks it faces — neither should it seek to do so, since risk taking is part of a company's raison d'être. However, it does need to establish a defensive armoury to protect its corporate reputation against the unforeseeable. Such an armoury would cover procedures, training, materials, and relationships. For example, procedures would include the establishment of a crisis management team; training

would cover aspects such as making skilled communicators available to relate with the media; materials might include policies and background briefs on
some of the more complex reputation risks; and relationships might include fostering“credit in the bank” among significant stakeholder groups.

Embedding the reputation risk process - In some respects, reputation risk should be treated in the same way as more traditional risks such as financial or operational risks. It should be included within a company’s internal audit procedures and kept up to date to avoid, detect and respond to reputation risks.

Perceptions and the internet

Reputation risk management differs from traditional risk management in an important respect: reputation is largely about perception. Many management teams have been criticized for the way they handled a crisis — not because their strategy was ill-conceived or clumsily implemented, but because they failed to tell the outside world what the strategy was.

The way a company handles a crisis is not only dependent on the quality and timeliness of its decision making but also on how its stakeholders perceive it. This is based on a blend of perceptions, which may pre-date the crisis. If a company has a reputation for putting profit before principle, it will face a tougher battle to protect its reputation. Companies that weather crises of reputation have often accumulated “credit in the bank” with the public and stakeholders.

Using the internet proactively enables a company to provide regular updates to all its important stakeholders. This need not only apply to external audiences but can apply internally through the corporate intranet. “Crisis centers” might make information available in real time, assisting those attempting to manage the situation. It can ensure that a single, current position statement is used by representatives in every market in which the company operates, reducing inaccuracy and inconsistency.

Philosophies of risk, shareholder value, the CEO and the Board

Risk is often viewed as a bad thing, yet shareholders pay companies to take risks in the hope of reaping benefits. It is necessary for the Chief Executive Officer [CEO] to formulate a philosophy of risk that considers both the traditional aversion to risk and the scientific approach of the risk manager. Such a philosophy will enable the CEO, alongside the Chief Risk Officer [CRO], to map out and implement specific risk policies in relevant areas of the business, and clarify the ways in which the company can best use risk to enhance shareholder value.

The bad news for CEOs is that despite a great expansion in the technologies and instrumentation of risk management, risk by its nature cannot be eliminated. The good news is that the CEO, not expected to remove risk – he is paid to take it, especially in the case of a bank, where the business of banking is primarily taking on risks.

Removing risk is potentially costly, but, more importantly, getting rid of risk stifles the source of value creation and upside potential. In fact, it may be in shareholders’ interests to encourage more

risk taking by CEOs. Since they are paid to take risks, they should not timidly look for ways to continuously pass them on to others.

Ultimate responsibility for risk lies with the CEO; it should therefore be part and parcel of his or her agenda at all times, not just when disaster strikes. This part of the article proposes that the CEO needs first to develop a clear philosophy of risk, and then formulate clear corporate policies to guide the management of risk. Such a discussion necessarily begins with the core elements of enterprise value.

The components of enterprise value

The core value of a quoted company could be thought of as having three components,

1. Tangible value - Tangible value reflects the bedrock of the real and tangible assets, which will sustain the firm's value in times of crisis. It is usually measured as book value. In recent times, tangible value has been degraded as the market valuations of dotcom "clicks and mortar" companies — with little book value but promises of great wealth — have outshone their "bricks and mortar" counterparts.

2. Premium value - Premium value represents the value in excess of book value at which the firm trades in the open market. This element of value is the source of a firm's competitive advantage. The value drivers here include, for example, the firm's reputation, its brands, intellectual property, innovation, potential growth, global reach, managerial expertise, and the skills and experience of the workforce. These intangible assets are a source of sustainable competitive advantage for a firm and enhance shareholder value.

3. Latent value - Latent value represents the potential or "hidden" value within a firm. Sources of hidden value might include the future potential of a merger, group synergies, operating efficiencies yet to be realized, under-promoted brands, an unmotivated workforce, innovation without patents, or managers in the wrong jobs. It is by realizing this source of value that the CEO can flourish.

Risk management is all about ensuring that enterprise value is enhanced and protected in a cost-effective manner and that latent value is realized. The biggest risk a CEO faces is that value is not created. The CEO must provide the leadership to face risk. This requires a personal philosophy of risk that is reflected in a clearly stated corporate policy. An event that could seriously damage enterprise value or prevent the realization of latent value should be identified, assessed, profiled, quantified, and considered for avoidance, containment or retention.

Enterprise risk and value.

Firms face a whole variety of different risk exposures. Each organisation will have a different risk landscape according to its business, objectives, financial structure, competitive position and operational spread.

Enterprise risk implies a view of risk in aggregate that is after the offsetting effects of individual

risk factors. However risk is generally not presented as an opportunity. In order to develop a sound philosophy of risk, the CEO must take a position on

(1) what the purpose of enterprise risk management is, and
(2) how much risk, the firm is prepared to take in the pursuit of opportunity.

Figure 1 illustrates a convenient classification scheme of enterprise risk factors and the three elements of enterprise value.

Figure 1: Enterprise risk

The value equation below illustrates the connection between risk and value.

$$\text{Enterprise value} = \underbrace{\frac{\text{Future cash flows}}{\text{Cost of capital}}}_{\text{[Tangible value]}} + \underbrace{\text{Growth opportunities}}_{\text{[Premium value]}} + \underbrace{\text{Latent value}}_{\text{[Latent value]}}$$

The various risk types are capable of affecting each element of the value equation. Risk policy needs to be grounded in an understanding of the way in which the key value drivers are affected by risk and the magnitude of the impact. This is intended to stand the Value at Risk (VAR) approach on its head. Ask not what value will be protected by removing risk, but what value will be created by retaining risk.

The CEO of the modern corporation is squeezed by the doctrinaire approach of risk avoiders and the apparently scientific approach of risk managers — hence the need for a philosophy of risk management. In short, the CEO needs to decide where to position the firm risk policy: in a performance context or in an avoidance context.

Developing a risk policy

Regardless of which philosophy of risk is adopted, a risk policy is crucial. The risk policy should deal in general terms with the objectives of risk management and the focus of responsibility.

The CEO should consider insurability as the critical factor in assigning responsibility for risk management. All insurable risks can be transferred to the markets in the form of insurance or derivative instruments. If a risk is not insurable, it is not “delegatable” and remains the CEO’s responsibility — it forms part of strategic risk management.

Market risk management represents the management of currency, commodity, and interest-rate risks, all of which are capable of being hedged in the short term. Hazard risk management deals with traditional and emerging event risks. Operational risk management deals with business structure approaches to containing risk. The hedging decision in each case will carry different risk and value implications for the firm.

Strategic risk - Significant parts of strategic risk cannot be diversified away. It is the responsibility of the CEO to manage this risk to the shareholders’ best advantage by exposing the upside and enhancing value. Exposures here include, for example, the risk to the firm’s reputation, the risks of managing investors’ perceptions and expectations, the risks of strong competition and erosion of competitive advantage, the risk of losing touch with your customers as well as with your own staff, and the risk of losing (either entirely or the potential of) the firm’s skilled staff.

Market risk - The corporate hedging policy plays an essential role in the broader risk policy. If a gold mining company, for example, were to hedge all its gold price risk, in effect it would remove all the downside risk and all the upside potential in one stroke. However, if the firm was battling for survival, and we assume for now that it has a responsibility to survive, then hedging might become a sensible strategy.

A reason often given for hedging is that it reduces uncertainty and the volatility of cash flows, but, from the shareholders’ perspective, this volatility may be acceptable (indeed, desired) and the price paid for hedging may produce a net result of value destruction. Alternatively, hedging might reduce the cost of capital, but where investors hold diversified portfolios and the firm encounters a stream of cash flows over many years, this argument is invalid.

Hazard risk - Hazard risks present some key differences from market risks. Generally, hazard risks are not tradable, their insurance operates by the principle of indemnity, and these contracts may be exposed to “moral hazard,” where the insured may affect directly the nature of the risk. However, the hedging rationale remains consistent with that for market risks. The premium paid for an insurance contract may be considered equivalent to the price paid for a levered security, or option. For the same reasons, hedging, or insurance purchase, can make sense for catastrophic risk, but otherwise is questionable from a value perspective. Even in cases of catastrophe, evidence of insurance coverage may be necessary, but is not sufficient to protect the firm’s share price from falling.

Operational Risk - Corporations may diversify operational risks by conducting business across many different industry segments and geographical regions. Research demonstrate that investors favor business focus over conglomeration, yet global spread over domesticity. These results are consistent with the idea that shareholders can diversify away industry risk more cheaply and easily than can managers, but still rely partially on managers to spread geographical risk, given the limited liquidity of some of the world’s stock markets.

The emerging role of the Chief Risk Officer (CRO)

A corporate view of risk must be defined before the firm's portfolio of exposures can be managed effectively. In reaching this definition, questions may be raised regarding the interplay of the risk exposures mentioned above. To what extent do they correlate with and compensate for each other? How does this classification help manage these inter-relationships?

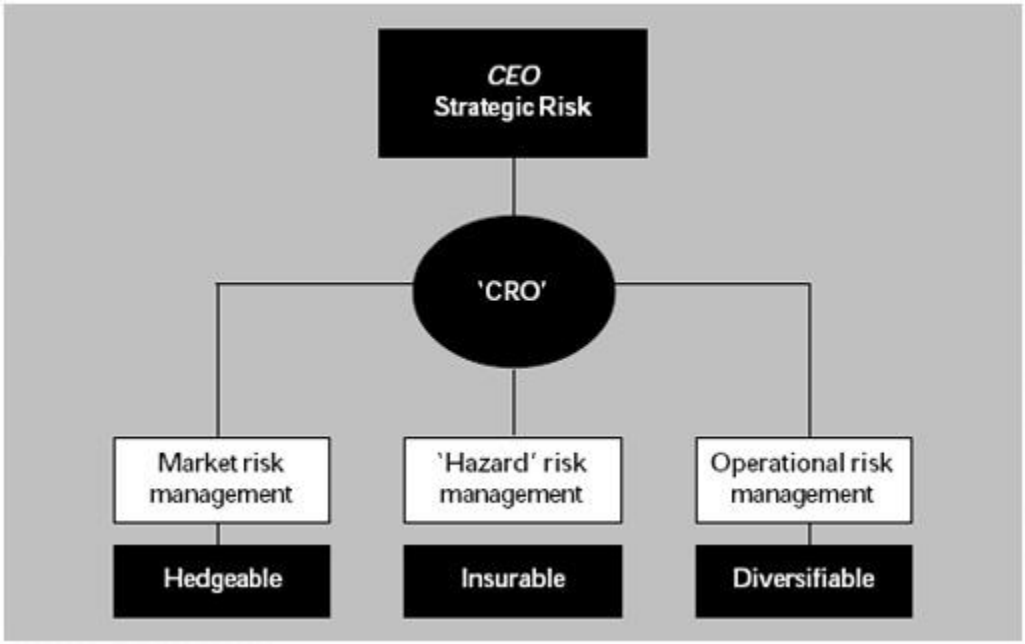
The delineation of responsibility for individual risks across the organization is the role of a CRO. The CRO should co-ordinate risk-related decisions and prioritize and communicate them to the CEO as a way of assisting with the formulation of risk policy. The diagram below illustrates the role of the CEO in risk management and the way in which responsibility for risk management can be delegated. In addition, it shows how insurable risks should be organized around the markets to which the risks can be transferred.

Risk policy guidelines

Having assigned responsibility, the risk policy needs to deal with a number of issues and provide the parameters within which risk management is to be executed. The CEO's risk policy requires guidelines in the following areas:

a) statement of objectives f risk management (philosophy of risk);
b) definition of risk classes;
c) assignment of responsibility for risk management;
d) hedging, insurance and diversification strategies;
e) use of instruments: disallowed instruments and financial limits;
f) risk reporting, including definition of financial limits, frequency and critical event reporting.

Figure 2 - Assignment of risk responsibilities



Risk management for the CEO is about two decisions:

- Whether to retain or hedge/transfer the risk; and

- Whether to provide or not for the retained risk.

Provision for the retained risk is used here to indicate a state of mind, rather than an accounting provision. The issue is about the extent to which the exposure should be allowed to affect the CEO's other decisions: financing, investment, dividend policy. Where exposures are provided for in an accounting sense, either explicitly on the balance sheet or implicitly by affecting other decisions, there often is a high opportunity cost of diverted capital. This, by its nature, destroys value. There is no perfect result of any risk analysis, but the CEO needs to know what the "default position" is, so that any deviation is informed and understood in value terms.

Developing a risk policy for the CEO is not a depressing task, full of reticence, warning and pessimism. It should be a creative initiative, exposing exciting opportunities for value growth and innovative handling of risk. The policy is not about compliance and disclosure, important as these may be. It is about developing a strategic approach to enterprise risks that releases value to shareholders. In the absence of such a policy, a company will be, at best, value-neutral; at worst, value-destroying. The risk policy provides the CEO with the impetus for sustainable value creation.

Risk management and internal control have moved firmly on to the boardroom agenda. It is argued that they should be an integral part of business and not a mere regulatory exercise. In the UK, the Turnbull report on internal control has provided companies with a framework for setting up robust systems of risk management. Board of Directors should identify and evaluate the risks that are specific to the achievement of their company's objectives. In doing so, they should consider emerging types of risk, such as those arising from branding and reputation as well as those in more traditional areas. Importantly, risk is not necessarily a bad thing; in fact, risk taking is an essential component of a competitive economy. Strategies for managing risk include acceptance, transfer, elimination, or control.

Risk management should be an integral part of every business and not just an exercise in meeting regulatory requirements. Evaluating and controlling risks effectively will ensure that opportunities are not lost, competitive advantage is enhanced, and less management time is spent firefighting. The likely reduction in surprises and the increased ability to meet objectives will strengthen shareholder confidence in the corporate business process. In time, this should lead to a higher share price and a lower cost of capital.

The Turnbull report, prepared by a working party of the Institute of Chartered Accountants in England and Wales and endorsed by the Stock Exchange, seeks to reflect best business practice by adopting a risk-based approach to designing, operating, and maintaining a sound system of internal control. The guidance, it offers comes in the form of a framework rather than a rulebook, and is planned so that each company can tailor the way it is applied to its specific circumstances. Thus, instead of specifying particular controls for all companies, the report calls on the boards of listed companies to identify risks that are significant to the fulfillment of corporate business objectives and to implement a sound internal control system to manage these effectively. To do this, the

board needs to be clear about the company's objectives — not just about what it is doing today but about its long-term strategic aims.

These guidelines encourage the management of risk, not its elimination. In a competitive market economy, a company with a low risk appetite is unlikely to generate a high rate of return. Indeed, in some cases a board-level review of the company's significant risks may lead to the conclusion that more opportunities need to be seized and greater risks taken, if the business is to succeed in the long run. However, directors and stakeholders must be aware that any risk management system can only provide reasonable assurance that a company's objectives will be met. The possibility of poorly judged decision making, human error, deliberate circumvention of controls, or unforeseen circumstances can never be ruled out.

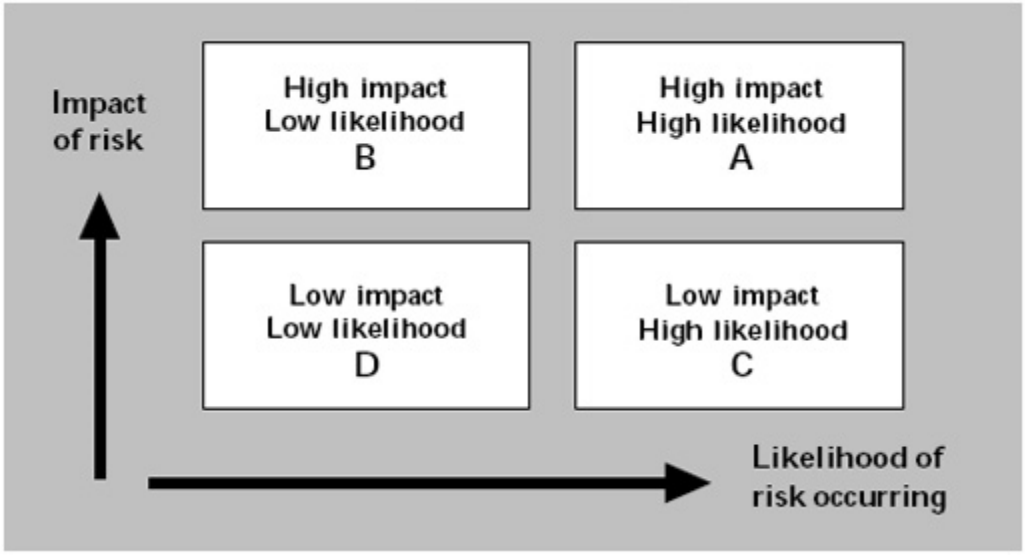
Identifying risks - When identifying risks, directors should be careful not just to select potential candidates from a generic matrix — the risks should be specific to the market sectors in which the business operates and to the company's circumstances at a given time. What are the possible obstacles standing in the way of the company achieving its business objectives? It will be helpful to look at how change, whether within the group or in the external business environment, is affecting the company's risk profile, as this can introduce new or increased risks.

It is important to consider problems or near misses that the company or its competitors have experienced recently, but managers should also address the types of risk that have yet to crystallize. Furthermore, consideration should be given to those business probity issues, including ones related to fraud, where the company might be especially vulnerable. With the development of global markets and worldwide brands, as well as the increased prominence of international pressure groups, many companies now find reputation risk a central cause of concern. In this context, environmental risks are substantial and growing for many sectors of business. These can lead to large direct costs, in terms of remedial expenditure and fines, and can severely damage corporate reputation.

Some significant risks are most easily identified from a "bird's eye" view at senior group level; others from more detailed operational knowledge further down the organization. The challenge is to bring these two strands together. As companies develop risk management systems, they find they need a common language throughout the group to describe similar risks, and common categories to classify them, so that the cumulative exposure in any given area can be properly assessed.

Prioritizing risks - Once identified, risks must be prioritized. This can be done initially by examining the "gross" risks associated with an event or situation. A gross risk is the probability of an event or situation occurring coupled with an estimate of its impact (before taking account of the application of control strategies). The potential impact should be assessed not merely in direct financial terms, but more broadly by reference to the potential effect on the realization of corporate objectives.

Figure 3 - How to prioritize risks



Some organizations use two-by-two diagrams (see Figure 3 above) to divide up risks.

Box A - shows risks requiring immediate action
Box B - those for which a contingency plan is needed
Box C - those for which action should be considered
Box D - those of lesser concern but nevertheless requiring periodic review

An embedded control system - Once gross risks have been prioritized, the directors need to decide in each case, their preferred control strategy for avoiding or mitigating these risks. They also need to identify those who are best placed to manage and account for them. Is it possible to design an early warning system? Such systems can identify problems before disaster strikes, when corrective action can still be taken. Once a control strategy has been agreed, the residual risk remaining in the business can be assessed.

There are various strategies for managing a given risk. These include

- accepting it
- transferring it partially or fully to another party (such as a through insurance or a joint venture)
- eliminating it by adopting an exit strategy
- controlling it through building safeguards into the operational process
- or ensuring that staff manage it

The Risk Mapping Process - Techniques for mapping risk have several common features.

Risk identification. Risk identification seeks to pin down all risks	quadrants, or a graph with two axes, representing levels of severity and

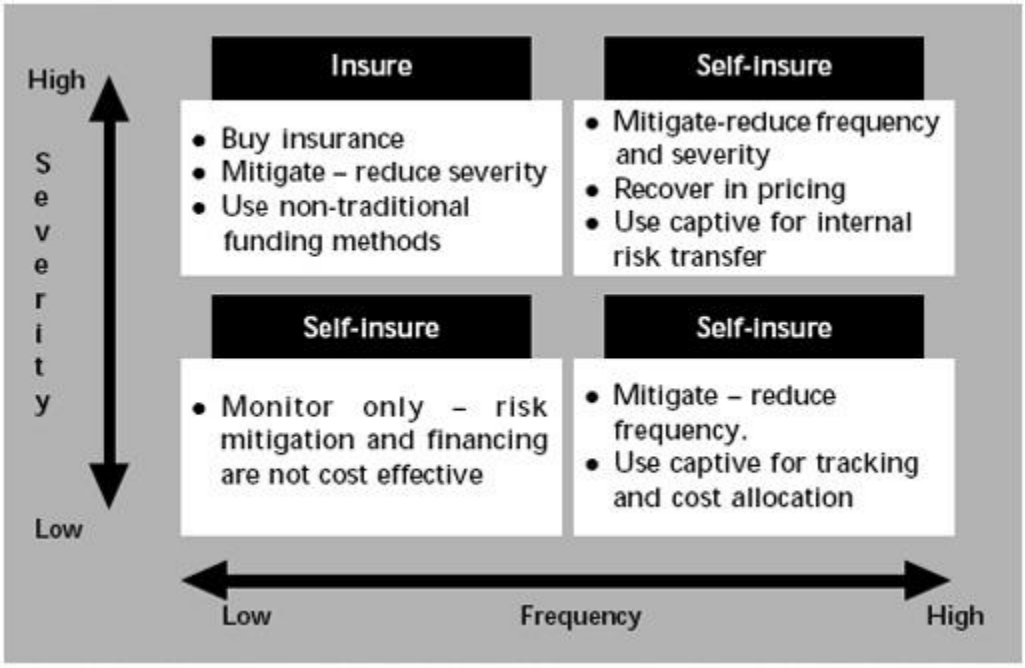
facing the business, from stationery theft to fraud, liability and fatality, without placing a value on these risks. In a top-down risk mapping process, risks are identified by examining publicly available information, conducting risk identification workshops with senior managers, or applying risk identification techniques to financial data. In a bottom-up process, workshops are held with middle and lower managers, with results aggregated up to board level.

Risk assessment.
Once risks have been identified, each is assessed for its frequency and severity. For instance, office stationery may often be stolen, but this risk may not be considered serious. On the other hand, the explosion of an oil rig may not happen frequently, but its consequences can be extremely severe.

Risk consolidation.
Once each risk has been identified and quantified, it can be placed on a risk map. Typically, this is a matrix with four levels of frequency. Each quadrant refers to a different category of risk, which needs to be handled differently (see Figure 3).

Risk portfolio management.
The final step in risk mapping is the most difficult. It requires managers to take an unconventional look at their businesses. Corporations present certain value propositions to investors. These might say: "Invest in the tobacco industry's strong cash flows," "Invest in Company's ability to choose good projects," or "Invest in the strong potential of this e-commerce business." Risk portfolio management therefore demands that executives have a good understanding of their group's value proposition with respect to the risk and return from each and every one of their businesses. They must see the set of businesses as a portfolio of risks that amounts to the value offered by its shares. They must actively manage the company's return relative to the capital it places at risk to obtain that return.

Risk map – the classic approach



A commonsense approach to enterprise-wide risk management

Total strategies for company wide risk control - Managers have always attempted to measure and control the risks within their companies. However, the enormous growth and development in both financial and electronic technologies have created a richer palette of risk management techniques. “Enterprise,” or “integrated,” risk management is a prime instance, offering an important new opportunity for increasing shareholder value. Integrated risk management is the identification and assessment of the collective risks that affect a company’s value, and the implementation of a enterprise-wide strategy to manage them.

The final frontier - The Financial Services Industry is fast learning that it should take a comprehensive approach to risk management. A piecemeal approach can miss significant risks or, worse, push risks into less visible places and create a misleading sense of safety. What is required is the application of consistent risk measurement techniques across various sources of risk. Organizational structures also need to be rearranged so as to give enterprise-wide risk authority to a single individual, or committee. The “silo” mentality of separately storing responsibilities for market, credit, and operational risks will no longer do.

The upside of this vast effort is an improved understanding of risks facing institutions. At a minimum, this will lower hedging costs, by pruning unnecessary transactions and taking advantage of diversification. At a more strategic level, the trend toward company-wide risk management will lead to better allocation of capital, taking into account not only rewards but also risks across business lines.

Sound Risk Management. - The ultimate test of the value of risk management effort is whether it enhances shareholder value. A full and proactive use of the tools of risk management significantly enhances value – not only those tools that help identify and evaluate risks, but also those that better inform management decisions **as to which risks to**

- hedge or mitigate,
- which to transfer or sell, and
- which to retain and capitalise

The discipline of risk management is still in a stage of development that lies between adolescence and young adulthood. In other words, there is great deal more to learn and we know less than we think we do.

This may be good news for practitioners, since there are many frontiers to explore, and it means there is substance to the adage that this is a discipline in which continuous improvement is necessary. On the other hand, it is a cautionary reminder to managers and regulators whose instincts are often to prescribe, codify and standardize risk management techniques. Experimentation, flexibility and diversity of methods are more in line with the current development stage of this discipline.

The analytical rigorous approach to risk measurement is one of the important attributes of a strong internal risk management effort. The other features would include

- The degree of transparency of risk
- The timeliness and the quality of information [MIS]
- The effectiveness of internal risk policies and controls
- The degree of line management and independent oversight
- The extent of diversification and avoidance of risk concentration and
- The judgment and experience of people

However, having said all this - risk models, analytical tools and reports alone cannot tell us about market dynamics; but would require the adoption of the following simple rules for effective risk management.

The 10 Simple Rules of Effective Risk Management.

1. There is no return without risk. Rewards go to those who take risk. Intelligent risk taking is to be encouraged by management, not stifled.

2. Be transparent. Risks need to be fully understood. A risk that is not understood is a risk that should be avoided.

3. Seek experience. Risk is measured and managed by people, not mathematical models. No new model is ever worth the sound judgment of an experienced risk manager.

4. Know what you do not know.
Every model is filled with assumptions. Know those assumptions, and actively question them.

5. Communicate. Risk needs to be discussed openly. A culture where people speak about their risks will be more successful than one that discourages an open risk dialogue.

6. Diversify. Multiple risks will produce rewards that are more consistent. Organisations get into trouble when one risk dwarfs all the other exposures they are taking on.

7. Show discipline. A consistent and rigorous approach will beat a constantly changing strategy. The temptation to change your goals, as market changes must be avoided.

8. Use common sense. It is better to be approximately right than precisely wrong. Do not spend your resources on improving the minutiae; concentrate on those issues that make the biggest difference.

9. Move with the change. Risks are evolving. Hence be open to move with changing times.

10. Get a Risk Grade. Return is only half the question. Make sure you have an accurate measure of the risk you are taking to assess

	accurately the true returns of your business.

Knowing when to say "No" - What matters most when you say "No" is that you have clear and understandable reasons to view a risk as inappropriate or excessive – since these are judgments, rather than fact, there will usually be differences of opinion. As a rule of thumb, we could distinguish between three generic reasons for viewing a particular risk as bad, each of which would offer different potential remedies.

a) The first is a risk for which there is no or grossly inadequate compensation. Examples include counterparty settlement risk in foreign exchange markets and many other forms of counterparty credit risk. In these cases, it is not a question of saying "Yes" or "No" to a risk. It is more a case of insisting that the risk be acknowledged and priced properly internally and the costs of the risk reflected against appropriate profit and losses.

b) The second type of reasons relates to one's judgment on a particular business unit's capacity to manage a risk. This involves several factors; the state of development of its internal risk control infrastructure, the degree to which the business enjoys a market leadership position, its familiarity and track record with managing similar risks; and its capacity to absorb mistakes, not in terms of its capital, but in its ability to hold to its business plan, keep people in place and make new investments, should it get the risk-taking decision wrong.

c) The third type of reason relates to judgment on the organisation's appetite and capacity to absorb risk. These are extremely complex judgments to make. They entail evaluation, not just of economic capital capacity, but also liquidity considerations, tolerance of earnings volatility, creditor and shareholder awareness of and tolerance of risk taking, management capacity to maintain business investment plans, and even, on occasion, regulatory acceptance.

Conclusion

Senior Management of Financial Institutions cannot afford to treat one of their most valuable corporate assets in a cavalier manner. Reputation risk should be managed with the same commitment as traditional risks. Generals do not wait until the battle is looming to build their defences. CEOs need to be similarly prepared.

Enterprise-wide risk management should, to a large extent be the concerns of all members within an organisation. As businesses evolve and grow, the incorporation of sound risk management culture into the organisation's business framework becomes crucial in ensuring continued success. Internally an organizational culture that incorporates good enterprise-wide risk management policies and practices promotes productivity. Senior management and business unit heads can focus more on their primary responsibilities instead of being distracted in to "fire-fighting", the problem that may arise due to the lack of such practices. Risk Management also strengthens the business planning process by allowing decision–makers to make contingency plans to avert possible "mishaps", thereby producing more realisable opportunities for the organisation on the whole and leading to increased shareholder value.

There are therefore significant economic and commercial incentives for establishing sound and effective enterprise-wide risk management control systems. Without such controls, an organisation

could, at best miss out on realisable opportunities, and at worst, be vulnerable to various risks that may annihilate the entire organisation in some instances. The presence of sound and effective risk management and control systems also inspire confidence in the investing public and counterparties. Beside protecting and enhancing shareholder value, it can also serve to safeguard the financial institutions credibility, goodwill, reputation and in the broader context, help to promote stability throughout the entire financial and economic system.

Finally, Risk Management is no rocket science – it is a basic common sense approach in managing your risks.

Quotes

- "Probable impossibilities are to be preferred to impossible probabilities" – Aristotle.
- "There are risks and costs to a programme of action but they are far less than the long range risks and costs of comfortable inaction" – John F Kennedy.
- "Prudent men in their dealings incur risks" – Vice-Chancellor Bacon (Re Godfrey -1883)
- "He is no wise man who will quit a certainty for an uncertainty" – Johnson.

References

1. The Boardroom imperative on internal control – by Anthony Carey and Nigel Turnbull

2. The emerging role of the risk manager – by Mark Butterswoth.

3. Value, risk and control; a dynamic process in need of integration – by Philippe Jorion.

4. Branding puts a high value on reputation management – by Bernd Schmitt.

5. Wise words and firm resolve when times get tough – by David Brotzen.

6. Issues of the moment; the rise and rise of risk management – by Ben Hunt.

7. Why risk management is not rocket science – by Rene Stulz

8. Reflection of a risk manager – by Stephen G. Thieke

9. Shareholder value and the CEO – by Rory F. Knight and Deborah J. Pretty.

Further reading

LMD Special Issue 2003/2004 – What's in a Brand ? - courtesy Brand Finance
(STING Consultants)

Buwanekabahu Perera

Buwanekabahu Perera is an Assistant Vice President at NDB Bank Ltd, attached to the Corporate Banking Department. He counts for 25 years' experience in banking in relation to Corporate Finance and International Trade Finance. He is an Associate Member of the Chartered Institute of Bankers, London [ACIB] and awaits election to associate membership of the Chartered Institute of Management Accountants [CIMA] - UK. Buwanekabahu also holds a Postgraduate Diploma in Bank Financial Management from Postgraduate Institute of Management, University of Sri Jayawardenapura.

He is a member of Association of Professional Bankers - Sri Lanka and its Secretary General since 2003.