Ranee Jayamaha: Governance, risk management and compliance

Keynote address by Dr Ranee Jayamaha, Deputy Governor of the Central Bank of Sri Lanka, at the Seminar on "Governance, Risk Management and Compliance and the Roadmap for Financial Services Industry", Colombo, 7 February 2008.

* * *

The Chairman and the Organizing Committee;

I would like to begin by expressing my gratitude for being given the opportunity to address a gathering that includes impressive groups of representatives from the financial services industry, risk management professionals, regulators and businesses.

As you are aware, the year 2008 has started off with the continuation of some of the challenges that resulted in significant disturbances in world financial markets: the impact of the sub prime market turmoil which originated in the US is still spreading across Europe and other financial markets; the Northern Rock crisis in the U.K. has raised serious regulatory issues; and the large frauds in global banks have highlighted the repercussions of the lack of internal controls and accountability in financial institutions. As in the past, many of these have been due to lapses in governance and risk management practices. Although Sri Lanka's financial markets have been insulated from these disturbances, they underscore the need for good corporate governance, better risk management and compliance in our financial industry. It is also important for us to learn from the bitter lessons experienced by others as our financial services industry too is tempted to provide low quality credit, which has been the root cause of the subprime issue.

The topic therefore is very relevant and it is time to generate a wider discussion on Governance, Risk Management and Compliance – in short – GRC, which are considered to be the three key pillars or imperatives of financial management.

1. What is GRC?

1.1 By itself, GRC is not new or unknown. GRC has always been of fundamental concern to businesses, the financial service industry and to regulators and supervisors. All stakeholders realize that there are enormous benefits of observing GRC and that such benefits would outweigh the cost of putting in place processes, procedures and controls that enable effective implementation of GRC.

1.2 Governance is all about self-discipline. It is the process by which the Board of Directors sets the objectives for an organization and oversees progress towards achieving those objectives. Put it simply, it is the set of procedures and processes that keeps the organization alive and allows it to operate as a "going concern". The higher the sophistication of the financial system, the higher would be the demand for governance as regulation and supervision cannot cover all risk elements in their supervisory processes.

1.3 The next critical pillar or imperative is Risk Management; i.e. identification, assessment, continuous monitoring of risks (real or hypothesized) and risk mitigation, while maximizing returns. In financial business, risk can emanate from many areas. The well-known risks are credit, liquidity, market, operational and human capital risks. There are several other risks, such as cross-border product risks, illiquidity risks etc. The new and complex products that are being offered by foreign financial markets or institutions can have cross-border risks as their distribution can bring in serious contagion risks across global markets. Most financial institutions do not view equity as risk capital. In banking, risks must include situations of drying up of liquidity. A case in point is the Northern Rock episode in which the bank exposed itself to the illiquidity risk. The need to bring in new capital to cover illiquidity was not given adequate attention by Northern Rock. Such risks should also be

analysed by banks and financial institutions and include them in their risk management framework. Ignoring this risk or not taking action to mitigate can be construed as the "moral hazard" we often speak about. Moral hazard leads banks and financial institutions to expect the public to rescue their institutions and continue to run on an illiquid basis, until they hit serious drying up of liquidity. If managed properly, risks can be confined to the institution concerned. If not, any one of these risks or a combination can affect a group of financial institutions or the entire financial services industry thereby creating a systemic risk. As Martin Wolf, a well known Financial Times journalist said "The financial services industry is famous for privatizing its gains and socializing its losses in that it expects the society at large to rescue them through public funds".

1.4 The third component is Compliance, which relates to laws and regulations, internal policies and procedures. Literally, Compliance means obedience or dutifulness, but it has broad scope and various interpretations. Compliance generally covers matters such as observance, application of standards of market conduct and managing conflicts of interests. More recently, Compliance has expanded its scope to cover specific areas such as operations of money laundering and terrorist financing and even tax laws that are relevant to financial services. In brief, the Compliance function should protect the institution against unlawful behaviour and strengthen its ethical consciousness. A Board of Directors of any financial institution should approve and oversee the institution's strategic objectives and set a compliance culture. Similarly, the Board should ensure that the financial institution has adequate policies and procedures that enable oversight activities to be carried out on all business lines. Given their fiduciary responsibilities, financial institutions, in particular, should comply with applicable laws and regulations in the jurisdiction in which they operate.

1.5 The word "Compliance" has also a connotation of regulatory and supervisory structures, which means that there is an external regulatory or supervisory body to ensure that financial institutions adhere to norms, guidelines and rules set by it. Compliance efforts will be effective and sustainable only in organizations where Compliance emerges from an ongoing board-level engagement. Compliance management therefore is the execution of business processes designed to manage risks and to continuously benchmark against expected parameters/tolerance levels applicable for the entire industry.

1.6 Compliance is considered to be costly, time consuming and an onerous endeavor. But, many financial institutions understand the criticality and the importance of better GRC and they are willing to devise strategies for leveraging their GRC systems to derive value as well as increase their compliance performance. Behind all these imperatives is the commitment at all levels to manage GRC in an integrated manner and inculcate the culture across the financial services industry.

1.7 The three GRC imperatives are interrelated in financial business and implementing them in isolation or treating them as separate elements would not be fruitful. In the past, most organizations have traditionally viewed, and some still continue to treat, GRC as separate components. The emerging perception of GRC is that it is an integrated set of concepts and, when applied holistically within an organization, it can add significant value and provide competitive advantage. Further, the holistic approach would be more efficient, consistent and legally sound and the Boards of Directors, senior management and staff at all levels would be involved in the organization's conduct of business. Most financial institutions have viewed GRC as discrete activities undertaken by different departments with no coordinated efforts. As a result, there is a lack of integration of GRC across business areas or functions.

2. New regulations and pressure for integrated risk management

2.1 During the past few years, regulatory and compliance requirements of the financial institutions have strengthened globally. Since the first updating of the Basel Capital Accord in the late 1990s, the Sarbanes-Oxley Act in 2002, the launch of new regulations seems to

have become more frequent. With these new requirements, financial institutions are facing an amplified focus on risk management with risk based performance measures and capital allocation. Rating agencies too have expanded their analysis of Integrated Risk Management practices when determining credit ratings.

2.2 The Financial Services Authority (FSA) in the UK, which has come under much criticism in recent times due to the failure of Northern Rock, has published its risk outlook report in 2008, which has identified 5 priority risks. Although some of these may not be directly relevant or applicable to Sri Lanka's financial institutions, they are common risks that need to be flagged by the Boards of Directors of financial institutions. The priority risks set out by the FSA are:

- Existing business model of some financial institutions are under strain as a result of adverse market conditions. Given the nature of financial business, i.e. borrow short term for funding longer term lending, it is irrational to assume plentiful liquidity to prevail at all times without treating liquidity as part of risk capital;
- Increased financial pressures may lead financial institutions to shift their efforts away from focusing on the conduct of business requirements and from maintaining and strengthening business as usual;
- Market participants and consumers may lose confidence in financial institutions and in the authority's ability to safeguard the financial system;
- A significant minority of consumers could experience financial problems because of their high levels of borrowings; and
- Tighter economic conditions could increase the incidence or discovery of financial crime or divert the institution's resources away from tracking financial crime.

2.3 In addition to these, there could also be institution specific risks, which may bring in potential disturbances. Conventional wisdom now is that the more recent episodes like Northern Rock were an accident waiting to happen as banking regulations have not been emphasizing on liquidity risks. The recent turmoil has exposed the vulnerability of a regulatory framework that places so much emphasis on how well capitalized a bank is, but makes little reference to whether it has an adequate cash cushion and liquid securities to see the institution through a period of market turbulence. In this instance, the Basel II regime also does not seem to offer much help.

2.4 Given these challenges in Risk Management, financial institutions are expected to move towards Integrated Risk Management (IRM) which, in simple terms, is a continuous proactive and systematic process aimed at understanding, managing and communicating risks from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives. In other words, IRM requires an on-going assessment of potential risks at every level and every segment and then aggregating the results at the corporate level to facilitate priority setting and improved decision-making. IRM should be embedded in the organization's corporate strategy and it should shape the organization's risk mitigation culture and highlight the importance of effective coordination among interdependent risks.

2.5 Many of you may have been following the rogue trading scandal that cost 4.9 billion Euros for Societe Generale – SocGen, the French Bank in recent months. The credibility of the bank suffered a fresh blow this week following the interim report handed over by the Finance Minister, Christine Lagarde to the Prime Minister. In summary, the findings of this report said "Very clearly, certain mechanisms of internal controls of SocGen did not function and those that functioned were not always followed by appropriate modifications". Further, the report highlighted 8 elements of internal controls that were clearly inadequate and they may have been the decisive factors behind the crisis. Some of the critical ones are: the security of the bank's IT systems and protection of logins; confirmation of all transactions

with all counterparties; respect for “Chinese Walls” between front and back offices; monitoring of cancellations and changes in trades coming from a single trader; and “atypical” behaviour such as failure to take holidays by Kerviel – the rogue trader.

3. Changes to the regulatory framework in Sri Lanka

3.1 Several new regulatory measures have been introduced to strengthen the regulatory and supervisory framework in Sri Lanka. In recent times, the Central Bank has moved away from compliance-based supervision to risk-focused supervision. In 2002, the Central Bank issued a voluntary code of governance for banks and financial institutions expecting them to improve their corporate governance. However, the introduction of this code did not show significant improvement at Board level, primarily due to lack of commitment by the Boards. The Central Bank’s regulatory examinations of banks and financial institutions have raised concerns on corporate governance, inadequate systems and controls, exposure to related party transactions, under-estimation of non-performing loans and inadequate provisioning for bad and doubtful loans, weak administration of loan accounts and potential credit risk and lapses in submission of periodical returns to the regulatory authorities. Almost all of these concerns are related to non-availability of a proper GRC processes in financial institutions. Considering the fiduciary responsibility of the Boards towards their stakeholders, and in the interest of wider financial system stability, the Central Bank issued directions on corporate governance in December 2007, requiring the banks to streamline their governance practices commencing from 2008.

3.2 The implementation of the Basel II framework from January 2008 is another enhancement to the regulatory structure, which requires the financial industry to have a better risk management framework. Most of the leading banks have set up independent risk management and compliance divisions to monitor bank-wide risks. These institutions should now focus in moving forward to implement advanced approaches under Basel II framework by setting up data warehouses and sophisticated IT systems in order to have better risk management and compliance. Similarly, the adoption of International Accounting Standards such as IAS 32 & 39 and IFRS 7, which deal with disclosures, presentation, recognition and measurement of financial instruments, also highlight the need for an integrated risk management, disclosures and compliance. There is, however, reluctance by banks to build robust IT infrastructure and advanced IT frameworks due to the high cost of investment and the time it would take to reap the benefits. It is important that banks and financial institutions change this mindset to pave the way for a GRC management and also to avoid operational losses due to product failures and frauds. Risks arising in these areas could spread beyond the financial institution concerned and have the potential to affect the entire industry.

4. Adopting an integrated GRC framework is a challenge

4.1 Understanding the demands of the organization’s stakeholders is the key in terms of performance and conformance, and aligning the organization to deliver against these objectives. Considering the risk appetite and risk tolerance of the organization, the processes and technology should be designed and deployed so that the achievement of objectives is measured, risks are assessed and continuous improvement is realized in support of effective GRC. Integrating GRC has become a challenge for virtually every financial institution looking to establish an integrated and consistent approach to controlling exposures, managing risks and creating value.

4.2 The major challenge in adopting an integrated GRC approach is the aligning of the GRC framework and processes to standalone and isolated solutions that are already in place. The difficulty is to integrate these isolated solutions through a flexible and add-on basis to embrace new requirements. Changing core business solutions without overhauling business requirements is considered to be a nightmare by many financial institutions. If it is

properly planned and designed, it would not be that bad and those who have taken the bold decision to do so will be the winners in the future.

4.3 Another important challenge would be to adopt a GRC framework, which is consistent with international standards. To enable this, new policies and procedures have to be written with links to automated systems. Keeping up with the international best practice is not an easy task, but we have much less choice in not doing so. It will also bring in new challenges for the supervisory and legislative community. The changes that occur at high speed, the new risks and complexities that cut across the financial industry at an international level may pose difficulties for institutions to be compliant at all times because their compliance today may not hold for tomorrow, but it is important to realize that today's challenges are tomorrow's history. So, it is necessary to act today.

4.4 Given the expansion of financial markets associated with rapid growth in India and China, it is essential for banking and financial institutions in the Asian region to analyze risks relating to innovative financial products that will be sold by these markets. In this regard, the wider financial system in Sri Lanka should be adequately robust and resilient to deal with complex risks associated with these new products. In this context too, Sri Lanka's financial services industry should focus on GRC as a package and deal with these three pillars or imperatives within an integrated framework.

4.5 Introducing an "awareness culture" of GRC is also a serious challenge. It is necessary to ensure that the integrated GRC should be a prime concern of the employees and the Boards, as well as the senior management of financial institutions. Continuous training of relevant stakeholders would be a solution to this challenge.

5. Key elements of a roadmap

5.1 Firm commitment to implement GRC as a package

5.1.1 The key to meet these challenges is the commitment by all stakeholders, i.e. the Boards of Directors, senior management and employees of the financial institution. The commitment has to be clearly demonstrated at all levels and not by isolated groups within the institution. Usually, commitment should commence at the top and filter down to all levels, which requires a well-coordinated effort. In designing a roadmap, one can begin by reviewing the situation and assessing associated risks. It would also be necessary to survey the existing GRC framework and identify gaps focusing on different procedures and processes that exist in organizations. All stakeholders should be convinced that the key GRC elements point towards the same goal and that there is little use in implementing these critical components in isolation. An integrated GRC package should then be designed ensuring that it relates to the business model of the financial institution and also taking into consideration the fiduciary responsibilities of financial institutions. Once each financial institution has designed its GRC framework, it would be easy to roll it out to the entire financial industry through various formal and informal institutions, which coordinates among different segments of the financial services industry. In our context, the Sri Lanka Bankers' Association, the Finance Houses Association, the Leasing Association etc., should be able to coordinate within and among their segments of the financial services industry in implementing GRC in an integrated manner.

5.1.2 If one financial institution experiences problems today, given the interrelated transactions, it could lead to a systemic issue which will result in the entire system suffering. Therefore, it is equally important to use peer pressure to get weak or prodigal institutions to comply with regulatory instructions and directives. So, it is everybody's responsibility to ensure that outliers are brought on to the desired path.

5.1.3 Clearly, training and consulting remain very important, especially to change the mindset to a more committed one. All stakeholders need to understand why GRC should be

implemented as a package and the benefits attached to it, from the point of view of the institution as well as its clients.

5.2 Leveraging on technology

5.2.1 Technology is a critical factor, which facilitates efficiency and effectiveness in the GRC processes. A real time risk, compliance and monitoring environment enables financial institutions to ensure that risks are being managed and disruptive events are being acted upon. Therefore, technology integration across the financial institution would enable institutions to gain more timely and reliable regulatory compliance, more efficient use of IT systems, and lower cost on development and maintenance of software applications. Many organizations that apply GRC best practices have understood that service-oriented architecture (SOA) is more appropriate, as it would promote GRC integration while securing the highest value that IT can offer. SOA is an architecture that provides IT infrastructure which allows different applications to exchange databases and participate in business processes that are loosely coupled from the operating systems and programming languages underlying those applications.

5.2.2 SOA is a design for linking business and computational resources that are available on demand to achieve the desired results to service consumers. Under SOA models, different applications/services can communicate with each other by passing data from one application/service to another, or by coordinating an activity between two or more applications/services. Further, the financial institutions with IT infrastructure based on stand alone systems acquired over time to meet different business goals can benefit from an integrated service-oriented architecture. Web services can be considered to implement a service-oriented architecture where certain functions/services can be accessible over standard Internet protocols that are independent from other IT systems in the institution. The Central Bank of Sri Lanka is now using a web-based application to gather regulatory compliance reports from financial institutions. Although it is still at a preliminary stage, it is certainly a step towards improving the quality of the GRC in banks.

6. Conclusion

6.1 Now is the time to change. There should be a multifaceted approach to face the GRC challenges. GRC should be treated as one package or a set. This approach includes governance, built on Principles and Rules, Integrated Risk Management Mechanisms to identify, assess and mitigate risks and a defined compliance mechanism that deals with internal and external compliance requirements. The financial institutions have the responsibility to establish a compliance mindset throughout the organization as a foundation that places high regard on ethics, trust and values. Energies that are used by some banks and financial institutions to design ways and means of flouting instructions and defying directives should be diverted to observance of governance and compliance.

6.2 I have highlighted the challenges that financial institutions could encounter in implementing GRC amidst ongoing increasing globalization, continuously changing laws and regulations, various forms of financial stresses and continuous evolution of complex financial products. These challenges underscore the importance of compliance and best practice, which have already been set by the financial services industry regulators and supervisors as well as the international standard setters.

6.3 In the present financial industry environment, where the stakeholders and other interested parties put pressure for greater transparency and corporate responsibility, the Board of Directors and senior management have to set high standards in all aspects of GRC. The increase in investments to improve the IT infrastructure and human resources to integrate GRC management can improve risk management as well as compliance performance and its efficiencies. The financial institutions that have strong governance and

compliance processes in an integrated GRC framework will be more capable of winning public confidence, attracting investors, improving corporate reputation and efficiency, as well as contributing to promote financial system stability.

6.4 Northern Rock's fall has become something of a parable for the times: a story of insecurity, mistrust and powerlessness that often seem to best describe some financial markets in our part of the world as well. It speaks to the fragility of the international financial system, which is directly impacted by globalization, of the capacity of the regulatory institutions and governments to shape events and the powerlessness of all stakeholders to halt an erosion of confidence in once solid institutions.

6.5 It is also important to note that markets and investors are much more vigilant than banks and financial institutions themselves. They may watch global events with bemusement or with justified suspicion and feel that nothing is straightforward anymore. We need to reduce such feelings in the public in our country and instill confidence in them. Given the severe impacts of the recent sub-prime crisis and low quality credit decisions in the US and Europe and large frauds in international banks, it is important that the financial services industry and the regulatory community reflect on what additional precautionary efforts should be initiated to ensure that Sri Lanka's financial services industry continues to function as a stable and resilient one. I hope that the deliberations of this seminar will lead to the preparation of a roadmap, which would help to promote a competitive, resilient and dynamic financial sector with new initiatives on Governance, Risk Management and Compliance.

Thank you.