THE ROLE AND IMPORTANCE OF RISK MANAGEMENT IN INTERNET BANKING

Mojtaba Mali
Young Researchers Club, Aliabad Katoul Branch, Islamic Azad University, Aliabad Katoul, Iran
Mojtaba_mali@yahoo.com

Hossein Niavand
Research scholar,in Statistics Department at University Of Mysore , India
mco.mailg@nddiavan

Farzaneh Haghighat nia
MSc of Financial Engineering Industrial Engineering and Management system Amir Kabir University of Technology, Tehran. F.haghigath88@yahoo.com

ABSTRACT:

Continuing technology developments and innovations are having significant impact on the way banks interact with their customers, suppliers and counterparties, and how they undertake their operations. Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks and other technology-related solutions to drive their businesses in an increasingly competitive domestic and global market. The internet in particular offers major opportunities for banks to reach new markets and expand the range of products and services they provide to customers. The very accessibility and dynamism of the internet brings both benefits and risks. The board of directors and management of a bank are responsible for managing its risks, including technology risks which are becoming more complex, dynamic and pervasive. The risk management process requires the board and management to review and appraise the cost-benefit issues on what and how much to invest in controls and security measures relating to computer systems, networks, data centers, operations and backup facilities. As a general principle, a risk management framework would require the following actions to be taken:

- Identify, classify and assess risks that are relevant to the bank's operations and systems.
- Develop a documented plan containing policies, practices and procedures that address and control these risks.
- Implement and regularly test the plan.
- Monitor risks and the effectiveness of the plan on an ongoing basis.
- Update the plan periodically to take account of changes in technology, legal requirements and business environment including external and internal threats and security vulnerabilities.

The aim of this set of guidelines is to require banks to adopt risk management principles and security practices which will assist them in:

- Establishing a sound and robust technology risk management framework.

- Strengthening system security, reliability, availability and recoverability.
- Deploying strong cryptography and authentication mechanisms to protect customer data and transactions.

All banks providing internet banking must erect a sound and robust risk management process that will enable them to identify, assess, measure and respond to technology risks in a proactive and effective manner.

The writer of this article is trying to look attentively and clarified the dimensions of selected subject by use of ″descriptive - analytic″ research method.

KEYWORDS: Risk Management, Internet Banking, measure, monitor, control.

1. INTRODUCTION

As banks rely increasingly on information technology and the internet to operate their business and interact with the markets, their awareness and recognition of the magnitude and intensification of technology risks should correspondingly be more perceptive and discerning, both for individual banks and the financial industry as a whole. In this networked and market-driven environment, it is critical that banks have flexible, adaptable and responsive operating processes as well as sound and robust risk management systems.

2. RISK MANAGEMENT FRAMEWORK

A sound and robust risk management framework requires the board and management to be responsible and accountable for managing and controlling technology risks. This responsibility calls for banks to perform risk
analysis by identifying information systems assets, determining security threats and vulnerabilities, estimating the likelihood of exploitation or attacks, assessing potential losses associated with these risk events and taking appropriate security measures and controls for asset protection. Risk analysis is the process of examining the technology infrastructures and systems to identify possible exposures and weighing the pros and cons of different risk mitigation actions.

This step requires an assessment of what damage might occur to the assets and from what sources or causes. Effective information system security controls are necessary for ensuring the confidentiality, integrity and availability of information technology resources and their associated data. These assets should be adequately protected from unauthorized access, deliberate misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure. Risks that are deemed material to the organization should be thoroughly evaluated and prioritized to enable a strategy to be developed for addressing and mitigating these risks.

3. TYPES OF INTERNET BANKING

Financial institution Internet offerings can be broadly classified into three groups with distinct risk profiles:

- Informational--Offers information about the bank's products and services ("brochure ware") and is low risk
- Communicative--Offers account-related information and possibly offers updates to static data (such as addresses). Since access is permitted to the bank's main systems, the risk is material.
- Transactional--Allows customers to execute financial transactions and carries the highest risk. Some transactional models carry higher risks, for example, if the customer has never visited a branch throughout his entire relationship and prefers to carry out all his transactions remotely (this commonly happens with some online share trading sites).

4. INTERNET BANKING RISKS

Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital.

4.1CREDIT RISK
4.2 INTERNET RATE RISK
4.3 LIQUIDITY RISK
4.4 PRICE RISK
4.5 FOREIGN EXCHANGE RISK
4.6 TRANSACTION RISK
4.7 COMPLIANCE RISK
4.8 STRATEGIC RISK
4.9 REPUTATION RISK

5. **THE RISK PLANNING PROCESS** is the responsibility of the board and senior management. They need to possess the knowledge and skills to manage the bank's use of Internet banking technology and technology-related risks. The board should review, approve, and monitor Internet banking technology-related projects that may have a significant impact on the bank's risk profile. They should determine whether the technology and products are in line with the bank's strategic goals and meet a need in their market. Senior management should have the skills to evaluate the technology employed and risks assumed. Periodic independent evaluations of the Internet banking technology and products by auditors or consultants can help the board and senior management fulfill their responsibilities.

6. IMPLEMENTING THE TECHNOLOGY

is the responsibility of management. Management should have the skills to effectively evaluate Internet banking technologies and products, select the right mix for the bank, and see that they are installed appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting

with a vendor who specializes in this type of business or engaging in an alliance with another provider with complementary technologies or expertise.

7. MEASURING AND MONITORING RISK

is the responsibility of management. Management should have the skills to effectively identify, measure, monitor, and control risks associated with Internet banking. The board should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. As part of the design process, a national bank should include effective quality assurance and audit processes in its Internet banking system. The bank Internet should periodically review the systems to determine whether they are meeting the performance standards.

8. CONCLUSION

The past few years have been characterized by rapid changes in technology and the introduction of corporate and retail banking services through the Internet. The unprecedented speed with which new technologies are being adopted, the ubiquitous and global nature of electronic networks, the integration of e-banking platforms with legacy systems and the increasing dependence of banks on third party information service providers, all dramatically amplify the magnitude of risks to which banks are exposed.

Many banks have assumed that Internet banking primarily increases information security risks and have not sufficiently focused on the effect on other banking-specific risks. Risk management disciplines have not evolved at the same speed and many institutions, especially the smaller ones, have not been able to incorporate Internet banking risk controls within their existing risk management structures.

- Internal Controls and Audit — Management should determine whether the controls and audit processes are adequate to enable the identification, measurement, and monitoring of risk associated with the Internet banking business.
- Legal Requirements — various legal requirements, including compliance issues, need to be understood before initiating an Internet banking business. Since many legal issues are undecided, management will need to monitor developments.
- Vendor Management — if the bank is researching outsourcers, the analysis should include consideration of potential vendors' financial condition, years in the business, and future plans.
- Contingency planning — whether provided by the bank or outsourcer, management should have an understanding of contingency planning as part of the due diligence process.
- Insurance — a review of insurance coverage may be in order especially if the hosting of the Web site has been outsourced.
- Consultants — the bank should ensure they have the proper level of expertise to make this business decision. The board and senior management may need to enhance their understanding of technology issues. If the expertise is not available in-house, the bank should consider engaging outside expertise.

REFERENCES

1. Abrams, C., Känel, J., Müller, S., Pfitzmann, B. and Ruschka-Taylor, S. (2006), "Optimized Enterprise Risk Management", IBM Research GmbH, RZ 3657.

2. Allen, L., Boudoukh, J. and Saunders, A. (2004), "Understanding Market, Credit, and Operational Risk: The Value at Risk Approach", Blackwell Publishing Ltd.

3. Bowling, D. and Rieger, L. (2005), "Risk Sense of COSO's New Framework for Enterprise Risk Management", Bank Accounting and Finance.

4. Culkin, N. and Smith, 'An emotional business: A guide to understanding the innovations of small business decision takers'. Qualitative Market Research: An International Journal D. 2000.

5. Directors & Trustees Digest (2005), GUIDANCE SEEKS TIGHTER RISK CONTROLS FOR INTERNET BANKING, Thursday.

6. Dyllick, T. And Hockerts, K. (2002), "Beyond the Business Case for Corporate Sustainability", Business Strategy and the Environment, 11:130-141.

7. Ganesh Ramakrishnan(2001), Risk Management for Internet Banking .

8. Hoyt, R., Moore, D. and Liebenberg, A. (2008), "The Value of Enterprise Risk Management: Evidence from the U.S. Insurance Industry", the Society of Actuaries.

9. Internet Banking--Comptroller's Handbook(1999), Comptroller of the Currency .

10. Kamiya, S., Shi, P., Schmit, J. and Rosenberg, M. (2007), "Risk Management Terms", University of Wisconsin-Madison, Actuarial Science, Risk Management and Insurance Department.

11. Liebenberg, A. and Hoyt, R. (2003), "The Determinants of Enterprise Risk Management: Evidence from the Appointment of the Chief Risk Officers", Risk Management and Insurance Review, 6(1): 37-52.

12. Matlay, H. and Addis, 'Adoption of ICT and e-commerce in small businesses (2003): an HEI-based consultancy perspective'. Journal of Small Business and Enterprise Development.

13. Monetary Authority of Singapore(2008), Internet Banking and Technology Risk Management Guidelines.

14. Nocco, B. And Stulz, R. (2006), "Enterprise Risk Management: Theory and Practice", Journal of Applied Corporate Finance, 18(4).

15. Onorato, M. (2005), "From Compliance to Value Creation: The Evolution of Enterprise Risk Management", Algorithmics.

16. Oracle (2009), "Risk Management: Protect and Maximize Stakeholder Value", An Oracle Governance, Risk, Compliance White Paper, February.

17. Pausenberger, E. and Nassauer, F. (2001), "Governing the Corporate Risk Management function: Regulatory Issues", In Risk Management: Challenges and Opportunities, Springer-Verlas.

18. Perrini, F. and Tencati, A. (2006), "Sustainability and Stakeholder Management: The Need for New Corporate Performance Evaluation and Reporting Systems", Business Strategy and The Environment, 15: 296-308.

19. Petravicius, T. and Tamosiuniene, R. (2008), "Corporate Performance and the Measures of Value Added", Transport, 23(3): 194-201.

20. Post, J. Preston, Lee, and Sachs, S. (2002), "Managing the Extended Enterprise: The New Stakeholder View", California Management Review, 45(1): 5-28.

21. Riley, B. (2009), "ERM-Capturing the Upside", Institute if Actuaries of Australia, Finity Consulting Pty Limited.

22. Risk Management Principles for Electronic Banking (2001), Basel Committee on Banking Supervision.

23. Rosenberg, J. and Schuermann, T. (2004), "A General Approach to Integrated Risk Management with Skewed, Fat-Tailed Risks", Federal Reserve Bank of New York, Staff Report No. 185.

24. Royer, P. (2000), "Risk Management: The Undiscovered Dimension of Project Management", Project Management Journal, ABI/INFROM Global, 31 (1): 6-13.