IRJC
International Journal of Marketing, Financial Services & Management Research
Vol.1 Issue 9, September 2012, ISSN 2277 3622

RISKS IN E-BANKING AND THEIR MANAGEMENT

PROF. VIRENDER SINGH SOLANKI*

*Institute of Productivity & Management,
Meerut.

ABSTRACT

Internet banking and other modes of e-banking have been a blessing for banking as far as speed, convenience and cost of delivery is concerned, but alongside it has brought many risks. It has also brought about a new orientation to risks and even new forms of risks. Technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures. E- Banking may soon convert from a complementary to the main provider of financial services and products. Consequently, a possible failure of a bank entering this sector can have various consequences on its future position in the market. The bank's strategy should be readjusted so that it meets the new challenges with risk balance.

KEYWORDS: E – banking, risks, operational, money laundering, cross borders, firewalls, customer education, auditing.

INTRODUCTION

The rapid spread of Internet banking all over the world is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels. However, internet is not an unmixed blessing to the banking sector. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting I-banking expose themselves. Regulators and supervisors all over the world are concerned that while banks should remain efficient and cost effective, they must be conscious of different types of risks this form of banking entails and have systems in place to manage the same. An important and distinctive feature is that technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures. Both evolve continuously. The thrust of regulatory action in risk control has been to identify risks in broad terms and to ensure that banks have minimum systems in place to address the same and that such systems are reviewed on a continuous basis in keeping with changes in technology.

THE RISKS

The growth of electronic banking has created a new basis with regard to the degree of exposure to the risk and therefore consequently the need of not only a differentiated regulating frame, but also mechanisms of monitoring to be formed, which has already begun to be shaped in the fields of Basle Committee of Banking Supervision.

The business risk is the risk of not being able to achieve the business targets due to inappropriate strategies, inadequate resources or changes in the economic or competitive

environment. It has to do with the ability the credit institution has in order to achieve the operational objectives by exploiting the available opportunities in the market. The big changes on the banking sector and the adoption of fast paced evolving technology also change the traditional strategic risks. A bank that will rush into the adoption of new technologies so that it is rendered pioneer is risking losing its investment as information systems lose their value in very short time interval. Moreover, there is the risk of extensive investment in particular products or services, which will not become acceptable by the end users. On the other hand, if it maintains a more conservative attitude there is the risk of becoming last, in an environment where the competition is moving fast and strengthens its place in the market. Internet banking may soon convert from a complementary to the main provider of financial services and products. Consequently, a possible failure of a bank entering this sector, can have various consequences on its future position in the market, especially when the competition of the banks, which are clearly connected with the I-banking and do not have any physical substance (virtual banks), is already given.

THE RISKS IN E-BANKING ARE AS FOLLOWS

- Operational risk
- Security risk
- System architecture & design risk
- Reputational risk
- Legal risks
- Money laundering risk
- Strategic risk
- Other risk

1. OPERATIONAL RISK

Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology. In most instances, e-banking activities will increase the complexity of the institution's activities and the quantity of its operations risk, especially if the institution is offering innovative services that have not been standardized. Since customers expect e-banking services to be available 24 hours a day, 7 days a week, financial institutions should ensure their e-banking infrastructures contain sufficient capacity and redundancy to ensure reliable service availability.

BANKS FACE THREE MAIN TYPES OF OPERATIONS RISK

(I) VOLUME FORECASTS

Accurate volume forecasts have proved difficult - One of the key challenges encountered by banks in the Internet environment is how to predict and manage the volume of customers that they will obtain. Many banks going on-line have significantly misjudged volumes. When a bank has inadequate systems to cope with demand it may suffer reputational and financial damage, and even compromises in security if extra systems that are inadequately configured or tested are brought on-line to deal with the capacity problems.

As a way of addressing this risk, banks should:

- undertake market research,
- adopt systems with adequate capacity and scalability,
- undertake proportionate advertising campaigns,
- Ensure that they have adequate staff coverage and develop a suitable business continuity plan.

In brief, this is a new area, nobody knows all the answers, and banks need to exercise particular caution.

(II) MANAGEMENT INFORMATION SYSTEMS

Banks may have difficulties in obtaining adequate management information to monitor their e-service, as it can be difficult to establish/configure new systems to ensure that sufficient, meaningful and clear information is generated. Such information is particularly important in a new field like e-banking. Banks are being encouraged by the FSA (Financial Services Authorities) to ensure that management have all the information that they require in a format that they understand and that does not cloud the key information with superfluous details.

Operational risk is the risk of incurring financial loss due to human or technical errors and fraud. Operational risk can arise from the failure to follow or complete one or more steps in the prescribed authorization process. Operational risk includes the risks associated with the failure of communications, the breakdown of data transport or processing, internal control system deficiencies, human errors, or management failure. As a result, the financial institution could experience delays or disruptions in processing, clearing, and settling retail payment transactions, that could lead to credit and liquidity problems at other financial institutions.

Operational risk can also arise from fraud. A financial institution's exposure to operational risk from fraud is the risk that a wrongful or criminal deception will lead to a financial loss for one of the parties involved. Currency and checks are more vulnerable to loss or direct theft, whereas fraud is the primary concern in bank card payment transactions.

Operational risk controls should include information system, procedural, administrative, and legal measures to prevent or limit financial loss as a result of operational risk. System measures include monetary and time limits (per transaction, per payment instrument, per

client), and personal authentication and encryption techniques to ensure the authenticity of the payer and transaction information integrity. Additional controls include the use of certified tamper-resistant equipment e.g., EFT/POS (electronic fund transfer/ Point of sales) terminals.

Procedural measures include appropriate dual custody and separation of duties for critical payment transaction processing and accounting tasks, payment data verification, clear error processing and escalation procedures, and confidential and tamper-resistant mailing procedures for bank cards and other sensitive material. Administrative measures should include IT audit coverage of operational controls, legal controls (including regulatory compliance and agreements), and personnel issues associated with staffing and training.

(III) OUTSOURCING

Finally, a significant number of banks offering e-banking services outsource related business functions, e.g. security, either for reasons of cost reduction or, as are often the case in this field, because they do not have the relevant expertise in-house. Outsourcing a significant function can create material risks by potentially reducing a bank's control over that function. Outsourcing is of course neither new nor unmanageable but banks should be mindful on outsourcing, which addresses these risks.

2. SECURITY RISK

Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc. A breach of security could result in direct financial loss to the bank. For example, hackers operating via the Internet could access, retrieve and use confidential customer information and also can implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, cost of repairing these etc. Other related risks are loss of reputation, infringing customers' privacy and its legal implications. Thus, access control is of paramount importance. Controlling access to banks' system has become more complex in the Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers.

In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank.

Unless specifically protected, all data / information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers' which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net.

Data residing in web servers or even banks' internal systems are susceptible to corruption if not properly isolated through firewalls from Internet. Proper access control and technological

tools to ensure data integrity is of utmost importance to banks.

Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system.

Non-repudiation involves creating a proof of communication between two parties; say the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects which are potential sources of risk. Banks should have:

1. A strategic approach to information security, building best practice security controls into systems and networks as they are developed

2. A proactive approach to information security, involving active testing of system security controls (e.g. penetration testing), rapid response to new threats and vulnerabilities and regular review of market place developments

3 Sufficient staff with information security expertise

4. Active use of system based security management and monitoring tools.

5. Strong business information security controls

3. SYSTEM ARCHITECTURE AND DESIGN RISK

Appropriate system architecture and control is an important factor in managing various Kinds of operational and security risks. A bank faces the risk that the systems it chooses are not well designed or implemented. For example, a bank is exposed to the risk of an interruption or slow-down of its existing systems if the electronic banking or electronic money system it chooses is not compatible with user requirements. Many banks are likely to rely on outside service providers and external experts to implement, operate, and support portions of their electronic money and electronic banking activities. Such reliance may be desirable because it allows a bank to outsource aspects of the provision of electronic banking and electronic money activities that it cannot provide economically itself. However, reliance on outsourcing exposes a bank to operational risks. Service providers may not have the requisite expertise to deliver services expected by the bank, or may fail to update their technology in a timely manner. A service provider's operations could be interrupted due to system breakdowns or financial difficulties, jeopardizing a bank's ability to deliver products or services. The rapid pace of change that characterizes information technology presents banks with the risk of systems obsolescence. For example, computer software that facilitates the use of electronic banking and electronic money products by customers will require updating, but channels for distributing software updates pose risks for banks in that criminal or malicious individuals could intercept and modify the software. In addition, rapid technological change can mean that staff may fail to understand fully the nature of new technology employed by the bank. This could result in operational problems with new or updated systems.

4. REPUTATIONAL RISK

Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship. It may be due to banks' own action or due to third party action. The main reasons for this risk may be system or product not working to the expectations of the customers, significant system deficiencies, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may cause customer-discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized.

Other reasons include losses to similar institution offering same type of services causing customer to view other banks also with suspicion, targeted attacks on a bank like hacker spreading inaccurate information about bank products, a virus disturbing bank's system causing system and data integrity problems etc.

Possible measures to avoid this risk are to test the system before implementation, backup facilities, contingency plans including plans to address customer problems during system disruptions, deploying virus checking, deployment of ethical hackers for plugging the loopholes and other security measures.

It is significant not only for a single bank but also for the system as a whole. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system. Thus the role of the regulator becomes even more important as not even a single bank can be allowed to fail.

5. LEGAL /COMPLIANCE RISK

Legal risk is the risk of non-compliance with legal or regulatory requirements. The legal risks are directly related to the electronic banking and they are increased as its use is extended. They mainly stem from the uncertainty that exists in the legal – regulative framework concerning the electronic banking. In most countries an explicit regulating framework does not exist and this is owed to the little experience regarding the sector of electronic banking. The problem becomes even bigger when a bank offers its electronic services to other countries as well, since a unified legal frame in international level does not exist. Each country puts its own rules into effect and it is difficult for a bank to constantly adapt its services and to be acquainted with all the laws that are in effect in every country.

Another legal risk is related with the protection of the customers' personal data. Bad use by the bank personnel or by exterior malignant intruders can expose a bank in serious legal risks. It is possible that the intruders acquire access in the databases of the banks and use the data of customers in order to commit a fraud. In this case a legal risk is created by the bad or not certified use of customers' data. The legal risks, in which the financial institutions will be exposed from the use of electronic banking, are expected to increase because of the uncertainty that characterizes the wider legal framework and the specific lawful regulations of transactions through an open electronic network as the internet is. The uncertainty with

regard to the validity of transactions, the protection of personal data, the involuntary consumer's exposure to foreign jurisdiction, the tax evasion, the laundering of money, the electronic fraud but also the legal responsibility in case a system collapses, increase the exposure to the legal regulatory risks.

In terms of the European Union, a regulating frame has been developed that is concerned with questions such as the electronic (digital) signatures, the distant rendering of financial services, as well as the Directive on the electronic commerce.

A customer inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions. In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer.

Compliance and legal issues arise out of the rapid growth in usage of e-banking and the differences between electronic and paper-based processes. E-banking is a new delivery channel where the laws and rules governing the electronic delivery of certain financial institution products or services may be ambiguous or still evolving. Specific regulatory and legal challenges include:

Laws and regulations governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and Reserve Bank of India continues to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships. Some of the legal requirements and regulatory guidance that frequently apply to e-banking products and services have been issued by R.B.I. in its notification on 14th June, 2001, which were the findings of a working group on Internet Banking. These guidelines are available on the web site of RBI.

6. MONEY LAUNDERING RISK

Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy. Money laundering is called what it is because that perfectly describes what takes place - illegal, or dirty, money is put through a cycle of transactions, or washed, so that it comes out the other end as legal, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income. Every financial institution is charged with the responsibility of developing policies and procedures to combat money laundering, which includes the duty to be aware of trends and adaptations in the methods by which money laundering is carried out. The most difficult aspect of this responsibility is a financial organization's ability to anticipate new criminal behavior and to proactively implement protocols before the criminal behavior occurs.

As Internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with "know your customer" laws.

To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, and conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

7. STRATEGIC RISK

On strategic risk E-banking is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not banking, skills can end up driving the initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks want or expect and may have unexpected implications on existing business lines.

Banks should respond to these risks by having a clear strategy driven from the top and should ensure that this strategy takes account of the effects of e-banking, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a clear business plan with an effective means of monitoring performance against it.

Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. Early adopters of new e-banking services can establish themselves as innovators who anticipate the needs of their customers, but may do so by incurring higher costs and increased complexity in their operations. Conversely, late adopters may be able to avoid the higher expense and added complexity, but do so at the risk of not meeting customer demand for additional products and services.

HERE ARE A FEW SIMPLE SECURITY TIPS TO KEEP IN MIND, FOR A SAFER ONLINE EXPERIENCE

- Do not provide any personal information. Be very suspicious of any e-mail from a business or person that asks for your password, passport number etc.
- Review the link provided to ensure it leads to a valid website.
- Review the sender's e-mail address to verify that it is from a valid e- mail account.
- Act quickly if you suspect fraud. If you believe someone is trying to commit fraud by pretending to be your bank, notify the financial institution immediately.
- Use a strong password.
- Change your PIN / password often.
- Do not visit suspicious sites. If you suspect that a website is not what it purports to be, leave the site immediately.
- Be alert for scam e-mails. These may appear to come from a trusted business or friend, but are actually designed to trick you into downloading a virus or jumping to a fraudulent website and disclosing sensitive information.

- Open e-mails only when you know the sender. Be especially careful about opening e-mails with attachments.

- Make sure your home computer has the most current anti-virus software. Install a personal firewall to help prevent unauthorized access to your home computer.

- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them.

8. OTHER RISKS

Traditional banking risks such as credit risk, liquidity risk, interest rate risk, and market risk may also arise from electronic banking and electronic money activities, though their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational, and legal risks. This may be particularly true for banks engaged in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in electronic medium.

CREDIT RISK

Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. The following aspects of on-line loan origination and approval tend to make risk management of the lending process more challenging.

- Verifying the customer's identity for on-line credit applications and executing an enforceable contract;

- Monitoring and oversight of third-parties doing business as agents or on behalf of the financial institution;

- Valuing collateral and perfecting liens over a potentially wider geographic area;

- Collecting loans from individuals over a potentially wider geographic area.

Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks engaging in electronic banking activities may extend credit via non-traditional channels, and expand their market beyond traditional geographic boundaries. Inadequate procedures to determine the credit worthiness of borrowers applying for credit via remote banking procedures could heighten credit risk for banks. Banks engaged in electronic bill payment programs may face credit risk if a third party intermediary fails to carry out its obligations with respect to payment.

LIQUIDITY RISKS

Liquidity risk is the risk arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses, although the bank may ultimately be able to meet its obligations. Liquidity risk may be significant for banks that specialize in electronic money activities if they are unable to ensure that funds are adequate to cover redemption and settlement demands at any particular time. In addition, failure to meet redemption demands in a timely manner could result in legal action against the institution, and lead to reputational damage.

INTEREST RATE RISK

It refers to the exposure of a bank's financial condition to adverse movements in interest rates. Banks specializing in the provision of electronic money may face significant interest rate risk to the extent adverse movements in interest rates decrease the value of assets relative to electronic money liabilities outstanding.

MARKET RISK

Market risk is the risk of losses in on- and off-balance sheet positions arising from movements in market prices, including foreign exchange rates. Banks accepting foreign currencies in payment for electronic money are subject to this type of risk.

BUSINESS RISKS

Business risks are also significant. Given the newness of e-banking, nobody knows much about whether e-banking customers will have different characteristics from the traditional banking customers. They may well have different characteristics e.g. I want it all and I want it now. This could render existing score card models inappropriate, thus resulting in either higher rejection rates or inappropriate pricing to cover the risk. Banks may not be able to assess credit quality at a distance as effectively as they do in face to face circumstances. It could be more difficult to assess the nature and quality of collateral security offered at a distance, especially if it is located in an area the bank is unfamiliar with (particularly if this is overseas). Furthermore as it is difficult to predict customer volumes and the stickiness of e-deposits (things which could lead either to rapid flows in or out of the bank) it could be very difficult to manage liquidity.

9. CROSS BORDER ISSUES

Electronic banking and electronic money activities are based on technology that by its very nature is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders, highlighting certain risks. Although banks currently face similar types of risks in international banking, it is important to note that these risks are also relevant to the cross-border conduct of electronic banking and electronic money. Banks may face different legal and regulatory requirements when they deal with customers across national borders. For new forms of retail electronic banking, such as Internet banking, and for electronic money, there may be uncertainties about legal requirements in some countries. In addition, there may be jurisdictional ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risk associated with non-compliance with different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules, and money laundering laws. Operational risk could arise for a bank dealing with a service provider located in another country, which for that reason may be more difficult to monitor.

RISK MANAGEMENT

For an increasing number of banks there may be a strategic reason for engaging in electronic banking and electronic money activities. In addition, greater use of electronic banking and electronic money may increase the efficiency of the banking and payment system, benefiting

consumers and merchants. At the same time, there are risks for banks engaging in electronic banking and electronic money activities. Risks must be balanced against benefits; banks must be able to manage and control risks and absorb any related losses if necessary. The rapid pace of technological innovation is likely to change the nature and scope of risks banks face in electronic money and electronic banking. Supervisors expect banks to have processes that enable bank management to respond to current risks, and to adjust to new risks. A risk management process that includes the three basic elements of assessing risks, controlling risk exposure, and monitoring risks will help banks and supervisors attain these goals. Banks may employ such a process when committing to new electronic banking and electronic money activities, and as they evaluate existing commitments to these activities.

RISK IDENTIFICATION AND ASSESSMENT

Risk assessment is an ongoing process in e-banking. It typically involves three steps. Firstly, Bank management should form a reasonable judgment of the magnitude of any risk with respect to both the impact it can have on the bank and the probability that such an event occurs. Management should determine the bank's risk tolerance, based on an assessment of the losses the bank can afford to sustain in the event a given problem materializes.

MANAGING AND CONTROLLING RISKS

Having made an assessment of risks and its risk tolerance, bank management should take steps to manage and control risks. This phase of a risk management process includes activities such as implementing security policies and measures, co-coordinating internal communication, evaluating and upgrading products and services, implementing measures to ensure that outsourcing risks are controlled and managed, providing disclosures and customer education, and developing contingency plans. Senior management should ensure that staffs responsible for enforcing risk limits have authority independent from the business unit undertaking the electronic banking or electronic money activity. Banks increase their ability to control and manage the various risks inherent in any activity when policies and procedures are set out in written documentation and made available to all relevant staff.

SECURITY POLICIES AND MEASURES

Security is the combination of systems, applications, and internal controls used to safeguard the integrity, authenticity, and confidentiality of data and operating processes. Proper security relies on the development and implementation of adequate security policies and security measures for processes within the bank, and for communication between the bank and external parties. Security policies and measures can limit the risk of external and internal attacks on electronic banking and electronic money systems, as well as the reputational risk arising from security breaches.

Security measures are combinations of hardware and software tools, and personnel management that contribute to building secure systems and operations. Such measures include, for example, encryption, passwords, firewalls, virus controls, and employee screening. Encryption is the use of cryptographic algorithms to encode clear text data into cipher text to prevent unauthorized observation. Passwords, pass phrases, personal identification numbers, hardware-based tokens, and biometrics are techniques for controlling access and identifying users.

Firewalls are combinations of hardware and software that screen and limit External access to internal systems connected to open networks such as the Internet. Firewalls may also separate segments of internal networks using Internet technology (Intranets). Firewall technology, if properly designed and implemented, can be an effective means of controlling access and safeguarding data confidentiality and integrity.

Although firewalls screen incoming messages they do not necessarily protect against virus-infected programs downloaded from the Internet. As a consequence, banks should develop prevention and detection controls to reduce the chance of virus attack and data destruction, particularly for remote banking.

INTERNAL COMMUNICATION

Aspects of operational, reputational, legal, and other risks can be managed and controlled if senior management communicates to key staff how the provision of electronic banking and electronic money is intended to support the overall goals of the bank. At the same time, technical staff should clearly communicate to senior management how systems are designed to work, as well as the strengths and weaknesses of systems. Such procedures can reduce operational risks of poor systems design, including incompatibility of different systems within a banking organization; data integrity problems; reputational risk associated with customer dissatisfaction that systems did not work as expected; and credit and liquidity risk. Concerned people must be provided the relevant training as technology advances.

EVALUATING AND UPGRADING

Evaluating products and services before they are introduced on a widespread basis can also help limit operational and reputational risks. Testing validates that equipment and systems function properly and produce the desired results.

OUTSOURCING

A growing trend in the industry is for banks to focus strategically on core competencies and rely on external parties specializing in activities outside the bank's expertise. While these arrangements may offer benefits such as cost-reduction and economies of scale, outsourcing does not relieve the bank of the ultimate responsibility for controlling risks that affect its operations. Consequently, banks should adopt policies to limit risks arising from reliance on outside service providers. For example, bank management should monitor the operational and financial performance of their service providers; ensure that contractual relations between parties, as well as the expectations and obligations of each party, are clearly understood and are defined in written, enforceable contracts; and maintain a contingency arrangement to change service providers in a prompt manner, if necessary. Security of the bank's sensitive information is of critical importance. The outsourcing arrangement may require the bank to share sensitive data with service providers. Bank management should evaluate the ability of the service provider to maintain the same level of security as though the activities were conducted in-house.

DISCLOSURES AND CUSTOMER EDUCATION

Programs to educate customers that address how to use new products and services, fees charged for services and products, and problem and error resolution procedures can help

banks comply with customer protection and privacy laws and regulations. Giving explanations and sharing the nature of a bank's relationship to a linked web site may help reduce legal risk to a bank arising from problems with services or products on the linked sites.

CONTINGENCY PLANNING

The contingency plan may address data recovery, alternative data-processing capabilities, emergency staffing, and customer service support. Backup systems should be tested periodically to ensure their continuing effectiveness. Bank management may insist that outside service providers have backup capabilities. In addition, management may consider compensating actions it can take in the event service providers become impaired.

MONITORING RISKS

For electronic banking and electronic money activities, monitoring is particularly important both because the nature of the activities are likely to change rapidly as innovations occur, and because of the reliance of some products on the use of open networks such as the Internet. Two important elements of monitoring are system testing and auditing.

SYSTEM TESTING AND SURVEILLANCE

Testing of systems operations can help detect unusual activity patterns and avert major system problems, disruptions, and attacks. Penetration testing focuses upon the identification, isolation, and confirmation of flaws in the design and implementation of security mechanisms through controlled attempts to penetrate a system outside normal procedures. Surveillance is a form of monitoring in which software and audit applications are used to track activity.

AUDITING

Auditing (internal and external) provides an important independent control mechanism for detecting deficiencies and minimizing risks in the provision of electronic banking and electronic money services. The role of an auditor is to ensure that appropriate standards, policies, and procedures are developed, and that the bank consistently adheres to them. An internal auditor should be separate and independent from employees making risk management decisions. To augment internal audit, management may seek qualified external auditors, such as computer security consultants or other professionals with relevant expertise.

MANAGEMENT OF CROSS BORDER RISKS

Cross border risks may be more complex than risks banks face within their home country. Hence, banks and supervisors may need to devote added attention to assessing, controlling, and monitoring operational, reputational, legal and other risks arising from cross border electronic banking and electronic money activities. Banks that choose to provide services to customers in different national markets will need to understand different national legal requirements, and develop an appreciation for national differences in customer expectations and knowledge of products and services.

CONCLUSIONS

- Internet banking has some inherent risks due to its nature. Legal system is still not very well defined across the globe, internet is prone to hackers and hence fraudulent risks are always there. The factor that technology is designed, driven and controlled by outside non bank people is a constant threat. The rapid pace of change of information technology presents the banks with the risk of system obsolescence and hence huge costs.

- In spite of the hardware and software technologies like firewalls, encryption and authentication there is risk perception in transactions particularly of high value.

- The legal position regarding information technology actions and crimes is still not very sound. Though after amending various exiting laws the IT act 2000 was passed but soon after the debate started and an amendment came in 2006 which was passed in a new act in 2008. Again there is a feeling that the laws around the globe are neither complete nor in perfect harmony as they should be as internet is a global medium.

- There is a risk of non bank organization emerging as banks through internet and start offering more lucrative facilities or virtual banks may come up without having any physical presence.

REFERENCES

- Agarwal, N., Agarwal, R., Sharma, P. and Sherry, A. M. (2003), E banking for comprehensive E Democracy: An Indian Discernment, Journal of Internet Banking and Commerce, Vol. 8, No. 1, June, 2003.

- Arunachalam, L. and Sivasubramanian, M. (2007) 'The future of Internet Banking in India', Academic Open Internet Journal, Vol. 20. Available online at: www.acadjournal.com

- Booz-Allen & Hamilton, Inc. (1997)."Booz-Allen's Worldwide Survey Revealed A Huge Perception Gap Between Japanese And American/European Banks Regarding Internet Banking." (http://www.bah.com/press/jbankstudy.html; current April 22 1997).

- Dasgupta, P. (2002), Future of E " banking in India, • available at www.projectshub.com

- DeYoung, R (2001b), The Financial Performance of Pure Play Internet Banks, Economic Perspectives 25(1): 60-75, Federal Reserve Bank of Chicago.

- Ganesan R, and Vivekanandan K, (2009) 'A secured hybrid architecture model for internet banking (e-banking)'. Journal of Internet banking and commerce, April, vol.14, no.1.

- Gupta, D. (1999) 'Internet banking: where does India stand?', Journal of Contemporary Management, December, Vol.2, No. 1

- Malhotra, P. and Singh, B. (2006, October–December) 'The impact of internet banking on bank's performance: the Indian experience', South Asian Journal of Management, Vol. 13, No. 4.

- Malhotra, P. and Singh, B. (2007) 'Determinants of internet banking adoption by banks in India', Internet Research, Vol. 17, No. 3.

- Rao, G. R. and Prathima, K. (2003) 'Internet Banking in India', Mondaq Business Briefing, 11 April.

- Ravi, V., Mahil, C. and Vidya Sagar, N. (2007) 'Profiling of internet banking users in india using intelligent techniques', Journal of Services Research, Vol. 6, No. 2 (October 2006)

- Reserve Bank of India (2001), Report on Internet Banking, at www.rbi.org.in.