Journal of Advances and Scholarly Researches in Allied Education
Vol. 15, Issue No. 12, December-2018, ISSN 2230-7540

Changing Profile of Indian Banking System and Modern Technology: Challenges & Issues

Dr. Kuldeep Singh[1]* Dr. Dalpat Singh[2]

[1] Associate Professor, School of Law, Manipal University, Jaipur

[2] Assistant Professor, Faculty of Law, Jai Narain Vyas University, Jodhpur

Abstract – A commercial bank is a financial broker in the Indian banking system that takes deposits of money from the government and loans them to benefit. A post office can take deposits but can't be considered a bank backing because it doesn't do a bank's other important feature, i.e. lending capital. Similarly, some other entities including Unit Trust of India (UTI), however cannot be termed banks because they do not allow checkable deposits. They are not banking finance firms1.

----------X----------

INTRODUCTION

The banking system is the cornerstone of an economy's finance market. The position of commercial banks in underdeveloped countries is especially significant. By mobilising capital and optimising their allocation, commercial banks play an important role in the underdeveloped countries' growth phase. Through attractive saving schemes and deposit security, commercial banks promote people's desire to save. By reaching out to people in rural areas, they help convert idle savings into effective ones. Commercial banks optimise capital distribution by lending resources to economic target sectors. These banks provide a meeting ground for the severs and the investors. Savers may not invest either because of inadequate savings and/or lack of risk-taking spirit[2].

Information Technology: Information technology (IT) has transformed the functioning of businesses, the world over. It bridged the holes in system coverage and distribution and enabled faster decision-making, based on up-to-date and exact details, lower costs and overall performance improvements. In India, the financial sector has become a major beneficiary of The Inroads in special banking. Many new banking and other financial intermediaries-based systems, goods and services are now IT-centered. Efficient technical convergence with sound market practises needs reengineering business processes and banks in India must follow up on the beginning of this phase. New distribution networks for customers—automated distributors (ATMs) and mutual payment networking for ATMs, internet bancing — and the launch of core banking solutions by most banks are some examples[3].

The RBI has played a proactive role in the implementation of IT in the banking sector. IT based initiatives are focused on meeting the three pronged objective of better house keeping, improved customer service and overall systemic efficiency. The RBI has established a vision plan for the Financial Sector, which details the strategy for IT adoption for the medium term of some three years. This paper would enable banks to finalise their IT plans in accordance with the RBI's overall approach in the banking sector.

E-Banking : Electronic Banking is a general concept that encompasses Online banking, tele-communications banking, telephone banking, etc. In other words, It is a process of delivery of banking services and products through electronic channels such as telephone, internet, cell phone etc. E-banking's and reach continue to grow.

The government of India and the Reserve Bank of India (RBI) have taken many steps to promote the growth of e-banking in India. As a regulator and supervisor, the RBI has made considerable progress in consolidating the existing payment and settlement systems, and in upgrading technology with to create an accessible, automated and healthy framework running in a real-time environment which has further contributed to the growth of e-banking in India. The Government of India adopted the IT Act, 2000, which gives legal recognition of electronic transactions and other forms of electronic commerce with effect from 17 October 2000.

Technology and Security Standards: The role of the netwnric and database is pivotal in securing te informtjon system of any organization Some of the important functions of the administrator viaa-vis system security are to ensure that only the Jatest version of the licenses software with latest patches are installed in the system, proper user groups with access privileges are created and users are

assigned to appropriate groups as pertheirbusiness role, a proper system of back up of date and Software is in effect and strictly adhered to, business continuity policies have been introduced and always reviewed and a reckoning mechanism is in place to record all network operations and to evaluate them[4].

Organizations should make explicit security plan and document it. There should be a separate system security. The Information Technology Division will actually implement the computer systems while the Computer Secutity Officer will deal with its security. The IS Auditor may review the information systems.

Access Control : On-date logical access codes, devices, programme applications, services, telephone cables, databases, device software, etc should be introduced. Logical access control technology can provide user authentication, passwords, smart cards or other biometric technology.

Firewalls : Banks can at least use the proxy server firewall form to avoid a direct link between the internet and the infrastructure of the banks. It enables a high degree of control and thorough inspection by logging and auditing software. For sensitive systems, a stateful inspection firewall is recommended which throughly inspects all packets of informatin, and past and present transactions are compared. These generally include a real-time security alert[5].

Isolation of Dial up Service : All the systems supporting dial up services through modern on the same LAN as the appliation server should be isolated to Previous network guidelines to circumvent the proxy server.

Security Infrastructure : PKI is the most common safe internet banking technology. It is not yet available, however. Although PKI infrastructure is highly advocated, the following options are recommended during the transition phase up to the introduction of the PKI infrastructure by IDRBT or government.

1. Usage of SSL to ensure the authentication of servers and the use of client-side certificates provided by the banks via a Certificate Server.

2. Usage of at least 128-bit SSL to protect browser contact on web servers and even encrypt confidential details such as passwords in transit inside the company itself6.

Isolation of Application Servers: Both unused services, such as ftp, telnet, on the application server are also proposed. The application server should be isolated from the e-mail server.

Security Log (audit Trail): Both device accesses should be logged, including incoming texts. Suspected or attempted entry to a device and compliance breaches should be recorded as well as follow-up measures taken under the Orgnization Escalation Procedure.

Penetration Testing: The information management officer and the information system inspector should run routine system penetration checks, including the following.

1. Try to formulate codes using password cracking software.

2. Find back door traps in the programmes.

3. Attempt to overload the system using DdoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.

4. Check if commonly known holes in the software, especially the browser and the e-mail software exist. –

5. The penetration checks may also be performed by external specialists (often referred to as 'Legal Hackers').

Physical Access Controls: While ignored in general physical access restrictions should be strictly applied. Physical protection can protect both communication networks and locations on which all internal and foreign risks are handled.

Back up and Recovery: The bank should provide a sufficient infrastructure and data backup schedules. The backup data should be regularly checked to ensure that transactions are recovered without loss in a time frame set out in the Bank's protection policies. Continuity in operation can be assured by emergency relief centres, where stored data is stored. This installation should also be routinely reviewed.

Monitoring against Threats: Banks can have software to track intrusions and assault devices and networks. These methods should be used routinely to avoid security violations.

Education and Review: Banks can periodically assess and optimise their security infrastructure and safety strategies in light of their own perceptions and changing technology. They should constantly train their security teams and end users.

E-Banking: E-banking is focused on technologies developed to extend the ' interactive' regional presence of banks and consumers without actually needing a corresponding real' extension. Such business growth will go beyond national bprders, which considerably raises the complexities of cross-border collaboration for bank supervisors through the following reasons.

1. The possible ease and speed at which banks worldwide can function with customers over interconnected electronic networks4 in places where a bank is not authorised or overseen.

2. The bank's capacity or non-willingness banks to use the network to cross boundaries and seamlessly connect banking operations, usually subject to non-banking oversight, which every financial market authority does not control.

3. The logistical difficulties that national authorities face in tracking or monitoring local links to e-banking pages that arise in other jurisdictions without cooperation of national authorities.

Banking organisations have been delivering services to consumers and businesses remotely for years. Transfers of electronic funds including small transfers and business cash management schemes, as well as freely available currency and retail account management machines are global features. However, delivering financial services over public networks such as the Internet is bringing about a fundamental shift in the financial services industry[7].

E-Banking Risks and Their Management: The usage of the internet as an additional supply source will change bank risk profiles to some extent and generate new problems for banks in risk management. The bank supervisors must also recognise the effect on the strategic danger, operating risk, reputational risk, legal risk, credit risk, liquidity risk, market risk and foreign-currency risk of the Bank's usage of the electronic banking channel.

1. Strategic and Business Risk: Strategic disruption is one of the most critical challenges to financial organisations' e-banking operations. Strategic risk is more common and more prevalent in nature, and varies from other risk groups. The strategic actions of the Managing Board and Senior Management of the Bank would influence all other types of risk.

Due to and consumer support and demand for e-banking and future efficacy, most banks would have to build a plan to utilise the internet access platform to provide consumers with information material and/or transactional services. The rapid changes in technology, the pace of competition with other banks and non-bank competitors and the nature of that strategy could expose banks to substantial risk if the planning and implementation of the strategy is flawed or otherwise not well thought through.

Some of the strategic risks involved with e-banking are directly linked with timing issues. There. There. The management decision to become a technology leader can be a big strategic danger, particularly if the organisation becomes burdened with systems made obsolete by rapid technologicaL change. Also, an overly conservative technology supporter cannot place himself appropriately in a crowded market or market that rapidly consolidates.

Operatiopal Risk: Because of the reliance on technology for all facets of ebanking opâational risk is one of the more significant risks. Banks should propose introducing an interconnected company-wide architecture and application framework to promote interoperability and reduce operational risk, ensure the security, integrity and availability of data and support the management of relationships with third-party. service providers.. Further, as technology, is also dramatically changing business models and operating processes, banks need to ensure that they have appropriate control procedures (including change control) and audit processes.

Reputational Risk: Any adverse progress that precludes the availability of their e-banking supply will harm the credibility of a bank. Banks have long based their business on a reputation of trust the ability to provide a trusted network to support c-banking is critical, and a bank's reputation can be damaged by Internet banking systems that are malfunctioning or otherwise alienating consumers and the public.

A bank's reputation can suffer if it fails to deliver secure, accurate and timely e-banking services on a consistent basis. A bank's reputation can also be adversely impacted if it fails to respond to inquiries posted via e-mail, does not provide proper disclosure, or violates customer privacy.

Hypertext links from a bank to third party web sites or outsourced serviàe providers may cause customer confusion about the provider of specific products and services offered, and whether they are insured or uninsured. Customers can 1so be confused about whether the links from the bank reflect an implied endorsement of the third party's products or services and may well look to the bank for recourse if problems are encountered.

Legal Risk: Legal risk arising from e-banking activities represents another area of increased concern. Currently, supervisors in every jurisdiction are examining how existing legal and regulatory frameworks originally designed to address issues affecting the "physical' The banking environment engages with the growth of the e-banking supply chain and explores future ambiguities.

A bank that establishes Internet connections with consumers in other jurisdictions can be unfamiliar with the laws and regulations on banking, consumer security and therefore may face higher legal risks. Even banks that do not intend to solicit business from consumers in foreign jurisdictions may find that their offerings on-line are considered solicitations in

some countries. For example, if a bank makes its Web site available in another language, regulators in any country where that language is spoken may determine that the bank is marketing services to its citizen and may find that the bank is therefore subject to its local laws and regulations.

Credit Risk: The credit risk of a banking institution can be affected by e-banking activities in a number of ways. Businesses, particularly small institutions, can very quickly grow by leveraging the Internet access channel that could contribute to increased asset quality and internal control threats. The use of the Internet also allows banks to expand their geographic reach out of their traditional area, which increases the challenge of understanding local market dynamics and risks, veritjing collateral and perfecting security liens with out-of- area borrowers. In addition, the Internet also makes it more difficult to authenticate the identity and creditworthiness of a potential customer, which are essenlial elements to sound credit decisions. [19] Further, there has been a tendency for some Internet-only banks to pay higher rates on deposits opened over the Internet, which could lead to a higher level of sub-prime credits at these institutions in order to support these higher deposit rates. These factors underscore the importance of sound credit underwriting policies, credit monitoring and administration practices regardless of which product delivery channel is used

Electronic Money (E-Money): In recent years, there has been a gradual switchover from the use of paper-based payments media to those based ‘on electronics. While the basic characteristics of these new instruments are by and large similar to those of paper-based instruments, the former present a different set of challenges to policy makers. Electronic money is one of these new items that has recently emerged on the Indian horizon[8].

Meaning of E-Money: E-money may be broadly defined as an automated store of monetary value in a technical system used to render transfers to entities other than the lender without including bank accounts necessarily in the transaction but as a prepaid bearer method. These goods may be categorised into two broad groups, namely. (a) the stored value card pre-payed (sometimes known as electronic pockets") and (b) the pre-Paid product dependent on software that utilises computer networks such as internet (sometimes known as digital cash" or "network money"). The stored value card method generally uses a plastic card microprocessor chip, while device-based solutions normally have advanced software mounted in a personal computer.

CURRENT ISSUES IN INDIAN BANKING

Despite substantial improvements in the banking sector, some issues have to be addressed over time as the reform process is entrenched further. The discussion on banking developments revolves around on a wide range of issues including the following.

1. Overall redrawing of boundaries between the State ownership of financial entities and private sector ones.

2. Public sector character of the banking sector and efficiency.

3. Dilution of the government stake and its impact on the performance of the banking sector.

4. Corporate governance in banks and other segments of the financial system.

5. Transparency of policies and practices of monetary and financial agencies and accountability.

6. Prudential requirements of market participants together with comprehensive and efficient oversight of the financial system.

7. Maintenance of best standards in accounting and auditing, as well as the compilation, production and distribution of symmetric.

8. Development Finance Institutions Significance (DFIs).

The commonality among these concerns has given rise to a wide recognition and acceptance of having a set of international standards and best practices that every systemically important country should strive to foster and implement[9].

SUMMING UP

The process of financial development in independent India has hinged effectively on the development of banking system. Financing of emerging trade and industrial activities during the 1 950s and the 1 960s reflected the dominance of banking as the critical source. Functionally, banks catered to the needs of the organised industrial and trading sectors. The primary sector consisting of agriculture, forestry, and fishing had to d on their own financing and on sources outside the commercial banks.

The most critical accomplishment of financial sector reforms has been a substantial improvement of the commercial banking sector's financial wellbeing, which is the most significant aspect of the Indian financial structure. Asset quality of commercial banks, which before the initiation of reforms, was at a very precarious level, improved significantly even as norms were tightened over the years and the economy slowed down. The capital position of commercial banks also improved significantly and

was somewhat higher than the prescribed level. Profitability of the commercial banking sector improved despite decline in spread, which itself is a measure of efficiency. Although the NPAs are still overwhelmed by commercial banks and low profitability as opposed to banks in other emerging market economies, the reforms have been effective in improving the output of commercial banks in terms of stability and productivity parameters.

REFERENCE:

1. Reserve Bank of India, Report on Currency and Finance, 2001-02 p. VI-I

2. Government of India, Planning Commission, Ninth Five Year Plan (1997-2002) Vol. I, p. 150

3. Hacking refers to the practice of breaking into a computer without authorisatin, for malicious reasons, just to prove it can be done, or for other personal reasons.

4. Attacks on internal systems including those by emp[loyees are more frequent than external attacks in many organisations.

5. Straight-through processing refers to automatic transaction processing without any humnan intervention in the transaction process flow.

6. A data warehouse is a large database of customer transactions, updated regularly, which is used as a source of information for data mining.

7. Government of India, Economic Survey, 2006-07, p. 63.

8. TCP/IP is a standardised communications protocol for transmiting data in packets via the Internet. TCP (Transfer Control Protocol) deals with the construction of the data packets, while IP (Internet Protocol) routes them from computer to computer.

9. Reserve Bank of India, Report on Currency and Finance, 2001-02 p. VI-16.

Corresponding Author

Dr. Kuldeep Singh*

Associate Professor, School of Law, Manipal University, Jaipur

alphaacare@gmail.com