



International Journal of Engineering, Business and Enterprise Applications (IJEBA)

www.iasir.net

Analysis of Risk Management of Vendor in Banking

Dr Hariharan.N.P¹, Reeshma.K.J²

¹Professor of Economics, ²Research scholar

^{1,2}School of Social Sciences and Languages,
VIT University, Vellore-14, Tamil Nadu,
INDIA

Abstract: Core banking across the globe has resulted in outsourcing of a number of activities of the banks. Vendors have come to stay in the banking industry. Though the vendors discharge a number of functions of the banks, they do not have accountability and do not own failures. Vendors provide banks with as much of comforts and also inconveniences. Banks have to develop measures to safeguard their interests and that of their customers. There have been guidelines globally as to how to deal with the vendors, and in India, there are specific guidelines given by RBI. The paper deals at length the risks associated with banks while dealing with vendors and suggests ways and means to mitigate the risks.

Keywords: Core banking, risks, outsourcing, investment banking.

I. Introduction

Before the introduction of economic reforms in 1990s, banking was a simple business like most other business of those years. With core banking, it has become impossible for the banks to manage the affairs with their own staff, because soft ware technology (an integral part of core banking) is not a strong point for an appreciable percentage of bank employees.

After the introduction of core banking, vendors have started playing major role in banking activities across the globe. With increasing dependence on vendors, the banks are taking risks. While third-party vendors may be developing the products or providing outsourced operations, the banks that hire them may be stamping these products and services with the bank's name. If a data breach occurs, a disruption to online banking services strikes or a product or service misfires, customers are likely to point to the bank, not the vendor.

II. Reasons for the Presence of Vendor

Financial institutions frequently use third-party vendors to reduce costs, enhance performance, and obtain access to specific expertise. Examples include outsourcing audits, compliance reviews, disclosure preparation, data processing, and website development. Financial institutions also use third-party vendors to offer products directly to customers. It is important to emphasize, however, that while day-to-day management of a product or service can be transferred to a third party, ultimate responsibility for all compliance requirements cannot be delegated and remains with the financial institution. Thus, institutions should recognize that using vendors involves significant compliance risk.

At many institutions, vendor-management programs have focused predominantly on risks to the bank and the financial system-specifically, on business continuity, financial strength, and credit risk. With the scope of regulatory oversight broadening to include the consumer, many firms are underprepared. But since financial institutions must bear the responsibility for their suppliers' misdeeds, they must improve the way they manage these relationships. In response to the changes, financial firms are looking for new solutions to identify and manage third-party risk. A number of leading banks and credit-card companies are developing and embracing best practices.

III. Global Guidelines

Operational Risks:

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme. As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems.

The first step in risk management is to identification, and measuring exposures to risk. There should be effective capital planning and monitoring programme. Risk exposures should be monitored and steps should be taken to

control or mitigate risk exposures. There should be periodical reporting to senior management and the board on the bank's risk exposures and capital positions.

Verification of the Framework is done on a periodic basis and is typically conducted by the bank's internal and/or external audit, but may involve other suitably qualified independent parties from external sources. Verification activities test the effectiveness of the overall Framework, consistent with policies approved by the board of directors, and also test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies.

Validation ensures that the quantification systems used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

IV. Guide lines by RBI

As a step towards enhancing and fine-tuning the risk management practices as also to serve as a benchmark to banks, the Reserve Bank had issued Guidance Notes on management of credit risk and market risk in October 2002 credit and market risk. 'Management' of operational risk is taken to mean the 'identification, assessment, and/or measurement, monitoring and control/mitigation' of this risk.

Highly Automated Technology: If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on integrated systems. SRAS automates and orchestrates enterprise IT security and risk management. SRAS simplifies and integrates network discovery, baseline configuration management and vulnerability management enabling reporting for enterprise risks and regulatory compliance. It offers flexible agent-based or agent-less data gathering options across multiple hardware and software platforms. SCAP validated, enterprise proven.

Emergence of E- Commerce: Growth of e-commerce brings with it potential risks (e.g. internal and external fraud and system securities issues) Some of the risks associated with e commerce are Copyright infringement and invasion of privacy suits stemming from digital scanning and morphing, Flight of intellectual property due to employees moving to competitors, electronic bulletin boards containing defamatory statements resulting in liability or embarrassment.

Internal Controls: Emergence of banks acting as very large volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems. The Basel Committee is distributing this paper to supervisory authorities worldwide in the belief that the principles presented will provide a useful framework for the effective supervision of internal control systems. More generally, the Committee wishes to emphasise that sound internal controls are essential to the prudent operation of banks and to promoting stability in the financial system as a whole. While the Committee recognises that not all institutions may have implemented all aspects of this framework, banks are working towards adoption.

The guidance previously issued by the Basel Committee typically included discussions of internal controls affecting specific areas of bank activities, such as interest rate risk, and trading and derivatives activities. In contrast, this guidance presents a framework that the Basel Committee encourages supervisors to use in evaluating the internal controls over all on- and off-balance sheet activities of banks and consolidated banking organisations. The guidance does not focus on specific areas or activities within a banking organisation. The exact application depends on the nature, complexity and risks of the bank's activities.

Outsourcing: Growing use of outsourcing arrangements and the participation in clearing and settlement systems can also present significant other risks to banks. The vendor landscape has over 50 large and small vendors. Large BPOs like WNS and Genpact traditionally catering to the international market are focusing on building their domestic BPO divisions. We have classified the vendor landscape in the domestic banking BPO into four categories:

- a) International leaders (established BPO vendors with strong presence in international BPO market like Mphasis)
- b) India leaders (primarily focused on domestic market like Aegis, InfoVision and Omnia BPO)
- c) Emerging companies (companies building capabilities and currently offering specialized services on a small scale like Caretel, vCustomer)
- d) 'Me-too' players (offering undifferentiated low value services)

Large scale multi-city operations, partnerships, ability to quickly ramp up operations while maintaining quality and developing advisory capabilities will be key success factors for outsourcing vendors focused on the banking industry. As per reports, with further de-regulation in the banking industry and entry of several new private and foreign banks, the addressable market for banking BPO is expected to grow to 10 times the current revenues.

V. Role of Investment banks

Large Scale Acquisitions, Mergers, de-mergers and consolidations test the viability of new or newly integrated systems. With increasing competitive pressures being placed on businesses and the trend towards globalization, companies are engaging more and more in M&A activity. Many companies looking to expand or streamline their business will use investment banks for advice on potential targets and/or buyers. This normally will include a full valuation and recommended tactics. The investment bank's role in mergers and acquisitions falls into one of either two buckets: seller representation or buyer representation (they are also called "target representation" and "acquirer representation").

Valuation: One of the main roles of investment banking in mergers and acquisitions is to establish fair value for the companies involved in the transaction. Investment banks are experts at calculating what a business is worth. They are also able to predict how that worth could be altered (i.e., what happens to the value of a company in a number of different scenarios and what those potential futures would mean financially). Financial models are constructed by investment banks to capture the most important fixed and variable financial components that could influence the overall value of a company. These models, depending upon the proposed transaction, can be extremely complex with special variables being added for special areas (i.e., there are different financial factors to consider in different sectors, countries, and markets when predicting or measuring a company's value). Because of their expertise in business valuation, investment banks can also provide the service of arbitrage opportunities for their clients. For instance, if a bank has performed valuation on a potential target company that suggests its market value (or the value of its shares in the marketplace) is less than what the business is actually worth, it may facilitate a merger or acquisition of this target company for its client that carries with it substantial profit opportunity.

Buyers versus Sellers: Investment banks do not just rely on buyers and sellers approaching them. They will also source deals by studying the market themselves and approaching companies with their own strategic ideas (i.e., they might suggest that two companies merge, or that one company acquires, or sells to, another). An investment bank that represents a potential seller has a much greater likelihood of completing a transaction (and therefore being paid) than an investment bank that represents a potential acquirer. This seller representation, also known as "sell-side work," is the type of advisory assignment that is generated by a company when it approaches an investment bank and asks it to find a buyer of either the entire company or part of its assets. Generally speaking, the work involved in finding a buyer includes writing a "Selling Memorandum" (a detailed sales document) and then contacting potential strategic or financial buyers.

Banks may engage in risk mitigation techniques: (e.g. collateral, derivatives, netting arrangements and asset securitizations) to optimize their exposure to market risk and credit risk, but which in turn may produce other forms of risk (e.g. legal risk).

VI. The New and Growing Risks

Vendor Risk Management guidelines are provided by Federal Financial Institution Examination council FFIEC. There are three key elements of risk in vendor relationship, they are:

1. Financial loss: may occur due to **Internal fraud.** (for example, international misreporting of positions, employee theft, and insider trading on an employee's own account), **External fraud.** (for example, robbery, forgery, cheque kiting, and damage from computer hacking), **Employment practices and workplace safety.** (for example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and generally liability), **Clients, products and business practices.** (for example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products), **Damage to physical assets** (for example, terrorism, vandalism, earthquakes, fires and floods), **Business disruption and system failure.** (for example, hardware and software failures, telecommunication problems, and utility outages), **Execution, delivery and process management.** (for example: data entry errors, collateral management failures, incomplete legal documentation, and unauthorized access given to client accounts, non-client counterparty mis-performance, and vendor disputes).

2. Loss of customer relation:

When the bank system fails, either due to negligence of the vendor or due to error, bank is ultimately held responsible. When the system of other banks works well, and if one bank has a failure, there is possibility for customer relations to fail and the customers migrating to other banks.

3. Time needed to replace vendor should the need arise:

When contract with a vendor is not yet over, but relationship between the vendor and the bank get strained, the bank may have to look for another vendor. This cannot be at a short notice, and depends on the size of the bank and the transactions that vendor was undertaking for the bank. If the bank is relatively small, change of vendor can be done without much delay. The same way of the vendor was only doing peripheral duties, change could be easily done. Normally for medium sized bank, change of vendor may take anytime between three to six months.

VII. Conclusion

To conclude, banks should follow a model by which the risks can be assessed. It can assist a bank through a software credit risk appraisal, data base regarding the required information. Banking risks arising through vendor mechanisms can also be addressed. With bank automation and core banking, vendors have come to stay in the banking industry, and banks should find out ways and means of minimizing the risks.

VIII. References

- [1] www.bis.org
- [2] www.rbi.org
- [3] www.sourcingnote.com
- [4] www.boundless.com
- [5] www.analyticsindiamag.com
- [6] www.crisil.com
- [7] www.idrft.ac.in