Risk Factor inherent in Online Banking

Dr. Naveen Sharma
COE and Associate Professor,
Suresh Gyan Vihar University, Jaipur
Email: Naveen.sharma@mygyanvihar.com

Manveer Singh Rajawat
Research Scholar, Department of Management, Suresh Gyan Vihar University, Jaipur
Email: Manveer1705@gmail.com

ABSTRACT
Online banking gives speed and convenience to banks. People use banking services anytime and from anywhere. They don't even need to visit bank premises which help customers to complete their task on one click instantly. It decreases cost of delivery but it also inherits risk with it[1]. Technology is a source but it is also a risky tool. Online baking will become main sources of financial product and services in future.

KEYWORDS: Online banking, risk, operational, liquidity, auditing.

I) INTRODUCTION: ONLINE BANKING

Online banking is welcomed all over it provides banking services economically. Users can do all their financial transaction on a secure website of bank. Internet is used as a proper channel for delivering banking services. Online banking offers much facility to users like: Account opening, Fund Transfer, Applying for credit cards and loans and paying them back, online shopping etc. key factor for success of online banking is adoption and Customer satisfaction[2].

Online banking help banking industry in reducing cost, for competitive advantages, to improve quality of financial services, to increase customer etc.

Online banking help user to perform their bank task 24*7 and from anywhere. They just have to visit bank website login there, and by entering their login credentials they can avail bank facility and perform their task. Online banking saves times of both banks and customers.

II) ADVANTAGES OF ONLINE BANKING

Advantages of online banking are:

1) It provides facilities 24*7.
2) Customer can avail banking facilities from anywhere.
3) Online banking facilitates in bill payment, money transfers etc.
4) It gives high speed than ATM, sites provides speed and confirm transaction termination.
5) Customer feels secure and confident while making transactions.

III) DISADVANTAGES OF ONLINE BANKING

Disadvantages of online banking are:

1) Application software are not so easy to access, especially the old age customer cannot use them.
2) Taking bank consent, filling the form and signed and on-site registration process is time consuming.
3) Some people are not so confident while making electronic transactions they feel paper work is more authentic.

IV) RISK IN ONLINE BANKING

Increase in Online banking has also increased risk which needs to be regulated and monitored. Some major risks involved in online banking are :

1) Operational risk: It's another name is transaction risk. It is actually a direct or indirect loss reason may be frauds, error while processing , inadequate information etc. Risk due to inadequate information include logical access to information, physical access to hardware, insufficient backup recovery etc. Risk can be in product as well as in services. If not properly planned, implemented and monitored online banking products are very risky. Banks should focus on providing accurate product. Customer should be little tolerant to errors.

This type of risk can be avoided by effective policies, procedures, and control over new risk exposures. It also includes duties segregation, reconcilements of Information security controls by adopting additional processes, tools, expertise, and testing[3].

2) Security Risk: There is a financial loss to bank when there is any unauthorized access to information system like risk management system, accounting system, etc occurs. Unauthorized access to bank system is very easy now as hacking is very easy. Hackers hacks system and can easily access, retrieve customer information. Virus can be implanted which results in loss of data, cost of repairing etc. There is also a risk to customer privacy and bank reputation.
   When customer demands service he must be identified first as this may be a source to risk. Bank should handle these problems. They should have: sufficient staff with technical expertise, strong business information security controls, and active use of system based security management and monitoring tools, a strategic approach to information security, building best practice security controls into system and network as they developed.
3) Reputational risk: when public opinion is negative it is a reputational risk. It leads to loss of customers and funding. Customer can be negative if he is not satisfied with product working, have insufficient product knowledge, he doesn't know the procedure to resolve the problem, if some other bank is providing same product but with more efficiency, data integrity problems, problem in network etc.
   To overcome this system should be checked before implementation, if system fails there should be a plan to address that, backup facilities, virus checking etc.
4) Money Laundering risk: It is hiding the identity, source and destination of the money. It is about converting black money to white money. Financial institution focus on developing policies and procedures to handle money laundering. Most challenging activity for financial institution is to change criminal behavior of the individual. Transactions occur locally in online banking, so bank is not able to apply traditional methods to avoid undesirable criminal activity or to prevent it.
   On this bank has to perform proper screening, has to apply customer identification techniques, has to do proper review of compliance, has to do audit trails, has to develop procedures and policies which can identify and report wrong task in online banking.
5) Legal/Compliance risk: When there is no compliance to legal requirements it leads to legal risk. Electronic banking increases legal risk. Every country should follow some regulatory framework as banks faces many problems in offering electronic transaction in absence of regulatory framework. There is a big problem when bank has to serve at international level (as every country has their rules which can change any time because of this banks faces many problems in adapting).there is one more problem related to protection of data. If unauthorized access to banks database occurs it lead to a legal risk.
6) System Architecture and Design risk: Appropriate system can manage operational risk. If system is not properly designed bank faces risk. Many banks takes help of outside service provider and external experts for online banking activity to implement, operate and support which exposes bank to operational risk. Service providers who deliver services are not so expertize they may fail to update technology.
7) Strategic Risk: Due to competition and upper pressure seniors introduce online banking to customers they even don't do the cost benefit analysis. This is a big bad decision. Better way to avoid this is by evaluating the risk and by evaluating the costs against potential return on investment while giving services.
   To avoid this banks should have knowledge of competition with other online services available, costs required in hiring staff for technical support which involves management of operating systems, web browser and communication devices.
8) Liquidity risk: It is a risk when bank is unable to meet short term financial demands. This mainly happens when bank is unable to convert hard asset to cash by not losing the capital or income. Online banking has a huge impact on liquidity risk and amount of deposits and loan is affected dynamically.
   To mitigate this risk bank should not only focus on impact of loan or deposit growth due to online market but also focus on the impact of such growth on capital ratios and potential increase in dependence on high rate deposit or low rate advances.

(V) TIPS FOR SAFER ONLINE EXPERIENCE

(i) The link should be checked properly to ensure about validity of website.
(ii) Use of strong password.
(iii) Password should be changed regularly
(iv) e-mails or messages seeking for personal information like password, passport number etc. should be avoided

(v) Surfing on suspicious sites should be avoided and If you find anything wrong quit that site.
(vi) Sender's mail address should be checked properly.
(vii) If fraud is detected, act quickly.
(viii) Attachment of mail should only be explore when the sender is known.
(ix) PC's should contain updated version of anti-virus.
(x) Bank and Credit Card transactions should be monitored regularly and cross checked with statement .

(VI) RISK MANAGEMENT

With increase in financial institution and technology, there is drastic increase in online banking activities which directly increases efficiency of banks. Due to online banking risk involved also increases. Risk is controlled and managed by banks and loses due to these risk are also absorbed. Banks should have process for responding the current risk and to cover the new risk. Three basic elements of risk management process are Risk Assessment, Risk Controlling and Risk Monitoring[4].

(VII) RISK ASSESSMENT

Risk assessment is ongoing process which includes identification of risk and assessment of risk. Firstly judgment of risk is made, impact and probability of risk is assessed and then loss is also assessed in case of occurrence of risk.

(VIII) RISK CONTROLLING

When risk assessment is done steps to control and manage risk is initiated.

Controlling risk included following points:-

(i) Internal Communication- There should be no communication gap between the upper level executives and staff. It should be clear to all that how the online banking and money is managed so that the target of the bank is attained. Staff should inform the upper level about system technicalities, its weakness and strengths. With this many risk can be controlled like operational, credit, liquidity and reputational risk.

(ii) Security Policies and Measures- security is about maintaining authenticity, integrity, operating processes and confidentiality of data. It wholly depends upon the process and measures taken for development and implementation, which limit internal as well as external attacks. Reputational risk occurs because of security breaches. There are many security measures like: firewall, encryption, password, employee screening and virus control.

(iii) Evaluating and Upgrading- Product should be properly evaluated and tested before it comes in market so that reputational and operational risk reduces.

(iv) Disclosures and Customer Education- some campaigns should be organized to educated customer about products and services, problems related to fees charged and error resolution should be cleared, customer protection and privacy laws etc.

(v) Outsourcing- Banks should check capabilities strategically and should bargain to external parties who are specialized which will in turn give benefits such as economies of scale, reduction in cost. Bank should opt for the policies so that risk due to external parties gets limited.

(vi) Contingency Planning- It includes customer service support, emergency staffing, data recovery and data processing capabilities. Backup systems should be checked regularly, in case they weaken compensating plans should be there.

(IX) MONITORING RISKS

With changes in the activities nature monitoring is needed[5]. Two factors of monitoring are system testing and auditing.

(i) System Testing- It detects system errors, unusual patterns, disturbance and attacks. Faults in security measures should be identified, isolated and confirmed by penetration testing.

(ii) Auditing- It minimize risk and detect deficiencies. Auditor is the person who develops policies and procedures. Internal auditor is always different from the employee that makes risk management decisions. External auditor is security consultants and professionals who supplement internal auditor.

(X) CONCLUSIONS

Online banking has intrinsic risk as hackers are prone to internet. People, who do not pertain to bank design, operate and command the technology so there is a continuous warning. Perception in transactions has high risk rather than hardware and software technologies like firewall, encryption and authentication. Non-bank organizations are occurring as banks through internet and providing better facilities this is also a risk. The IT crimes laws are not sound.

REFERENCES

1. Ms. Sapna Kumari et.al., “RISK FACTORS AND SECURITY ISSUES INHERENT IN ONLINE BANKING”, IJARIIE-ISSN (O)-2395-4396, 2007, Volume 3, Issue 4.
2. Prof. Virender Singh Solanki, “RISKS IN E-BANKING AND THEIR MANAGEMENT”, International Journal of Marketing, Financial Services & Management Research Volume1, Issue 9, September- 2012, ISSN 2277 3622.
3. Teju Kujur et.al., “Electronic Banking: Impact, Risk and Security Issues”, International Journal of Engineering and Management Research, Volume-5, Issue-5, October-2015, Page Number: 207-212
4. Solanki V., “RISKS IN E-BANKING AND THEIR MANAGEMENT”, International Journal of Marketing, Financial Services & Management Research, 2012, Volume1, Issue 9.
5. Hole et.al., “An Analysis of the Online Banking Security Issues”.
6. MS. Sapna kumari and Ms. Vinita choudhary,” RISK FACTORS AND SECURITY ISSUES INHERENT IN ONLINE BANKING”, IJARIIE, 2017, volume 3, issue 4.
7. Phaninee Naruetharadho et.al., “FACTORS AFFECTING SUSTAINABLE INTENTION TO USE MOBILE BANKING SERVICES”, SAGE Open,2021, DOI: 10.1177/21582440211029925.
8. Hoang Ba Huyen LE,” Factor Affecting Customers’ Decision to Use Mobile Banking Service: A Case of Thanh Hoa Province, Vietnam”, Journal of Asian Finance, Economics and Business,2020, Volume 7, Issue 2.
9. V Vimala, “AN EVALUATIVE STUDY ON INTERNET BANKING SECURITY AMONG SELECTED INDIAN BANK CUSTOMERS”, Amity Journal of Management Research, 2016, Volume 1, Issue 1.
10. Khare A., “ONLINE BANKING IN INDIA: AN APPROACH TO ESTABLISH CRM”, JOURNAL OF FINANCIAL SERVICES MARKETING,2010, volume 15.
11. Zhao A. L. et.al, “ADOPTION OF INTERNET BANKING SERVICES IN CHINA: IS IT ALL ABOUT TRUST?”, International Journal of Bank Marketing, 2010, volume 28, Issue 1.
12. Kamakodi, N., & Khan, B. A., “CUSTOMER AND SERVICE LEVEL IN E – BANKING ERA: AN EMPIRICAL STUDY”, The ICFAI University Journal of Bank Management, 2008, volume 7, Issue 4.