RISK MANAGEMENT OF E-BANKING ACTIVITIES

Virlanuta Florina

"Dunarea de Jos" University Galati, Economic Science Faculty, florinaoana27@yahoo.com

Moga Liliana

"Dunarea de Jos" University Galati, Economic Science Faculty, liliana.moga@gmail.com

Ioan Viorica

"Dunarea de Jos" University Galati, Economic Science Faculty, ioan.viorica@ugal.ro

Summary: E-banking 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. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

Keywords: e-banking, risk management, security

1. E-banking risks

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet or mobile phone. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone.

In Romania, over 23 banks implemented and offer now e-banking services. The continuous development of the supporting technology, information security and e-banking strategy reflects on the increasing number of the e-banking customers. According to Communications and Information Technologies Ministry, the number of e-banking users and the transactions performed in this system, as well as the value of these transactions, registered a spectacular rising, displayed in the graphics below:

Year Index	2004	2005	2006	2007
E-banking customers	18.259	44.538	100.799	187.471
Transactions number	1.968.170	2.244.067	3.546.549	4.851.427
Transactions value (euro)	7.911.987.706	11.566.348.720	20.510.170.662	44.830.322.635

Source: Communications and Information Technologies Ministry

While the risks and controls are similar for the various e-banking access channels, this essay focuses specifically on Internet-based services due to the Internet's widely accessible public network. Accordingly, this project begins with a discussion of the two primary types of Internet websites: informational and transactional. Informational websites provide customers access to general information about the financial institution and its products or services.

Risk issues examiners should consider when reviewing informational websites include: Potential access to confidential financial institution or customer information if the website is not properly isolated from the financial institution's internal network; Potential liability for spreading viruses and other malicious code to computers communicating with the institution's website; and Negative public perception if the institution's on-line services are disrupted or if its website is defaced or otherwise presents inappropriate or offensive material.[2]

Transactional websites provide customers with the ability to conduct transactions through the financial institution's website by initiating banking transactions or buying products and services. Banking transactions can range from something as basic as a retail account balance inquiry to a large business-to-business funds transfer. E-banking services, like those delivered through other delivery channels, are typically classified based on the type of customer they support. The following table lists some of the common retail and wholesale e-banking services offered by financial institutions.

Since transactional websites typically enable the electronic exchange of confidential customer information and the transfer of funds, services provided through these websites expose a financial institution to higher risk than basic informational websites. Wholesale e-banking systems typically expose financial institutions to the highest risk per transaction, since commercial transactions usually involve larger dollar amounts. In addition to the risk issues associated with informational websites, examiners reviewing transactional e-banking services should consider the following issues:

- Security controls for safeguarding customer information;
- Liability for unauthorized transactions;
- Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures

2. Transaction risk

Transaction 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 transaction/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. Even institutions that do not consider e-banking a critical financial service due to the availability of alternate processing channels, should carefully consider customer expectations and the potential impact of service disruptions on customer satisfaction and loyalty.[1]

The key to controlling transaction risk lies in adapting effective polices, procedures, and controls to meet the new risk exposures introduced by e-banking. Basic internal controls including segregation of duties, dual controls, and reconcilements remain important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. However, management should consider additional precautions when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels.

Funding and investment-related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The Internet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits. But Internet-originated deposits have the potential to attract customers who focus exclusively on rates and may provide a funding source with risk characteristics similar to brokered deposits. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence.

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. Laws governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and banking agencies continue to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships.

Institutions that offer e-banking services, both informational and transactional, assume a higher level of compliance risk because of the changing nature of the technology, the speed at which errors can be replicated, and the frequency of regulatory changes to address e-banking issues. The potential for violations is further heightened by the need to ensure consistency between paper and electronic advertisements, disclosures, and notices.

3. Risk management

E-banking has unique characteristics that may increase an institution's overall risk profile and the level of risks associated with traditional financial services, particularly strategic, operational, legal, and reputation risks. These unique e-banking characteristics include: Speed of technological change, Increased visibility of publicly accessible networks, Less face-to-face interaction with financial institution customers. Management should review each of the processes discussed in this section to adapt and expand the institution's risk management practices as necessary to address the risks posed by e-banking activities.

Financial institution management should choose the level of e-banking services provided to various customer segments based on customer needs and the institution's risk assessment considerations. Institutions should reach this decision through a board-approved, e-banking strategy that considers factors such as customer demand, competition, expertise, implementation expense, maintenance costs, and capital support. Some institutions may choose not to provide e-banking services or to limit e-banking services to an informational website.

Financial institutions should periodically re-evaluate this decision to ensure it remains appropriate for the institution's overall business strategy. Institutions may define success in many ways including growth in market share, expanding customer relationships, expense reduction, or new revenue generation. If the financial institution determines that a transactional website is appropriate, the next decision is the range of products and services to make available electronically to its customers. To deliver those products and services, the financial institution may have more than one website or multiple pages within a website for various business lines.

Financial institutions should base any decision to implement e-banking products and services on a thorough analysis of the costs and benefits associated with such action. Some of the reasons institutions offer e-banking services include: Lower operating costs, Increased customer demand for services, and New revenue opportunities.

The individuals conducting the cost-benefit analysis should clearly understand the risks associated with e-banking so that cost considerations fully incorporate appropriate risk mitigation controls. Without such expertise, the cost-benefit analysis will most likely underestimate the time and resources needed to properly oversee e-banking activities, particularly the level of technical expertise needed to provide competent oversight of in-house or outsourced activities.

Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods. While the details of any control and the effectiveness of risk mitigation depend on many factors, in general, each financial institution with external connectivity should ensure the following controls exist internally or at their TSP.

Conclusions

A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. 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. In managing the strategic risk associated with e-banking services, financial institutions should develop clearly defined e-banking objectives by which the institution can evaluate the success of its e-banking strategy.

Bibliography

1. Alexandra Horobet, Risk Management, Editura CH BECK, 2005
2. World Bank, Banking Risk Management, IRECSON,2006
3. WWW.MCTI.RO