E-Banking: Risk Management Practices of the Estonian Banks

Dmitri Sokolov
Institute of Economics at Tallinn University of Technology
101 Kopli Street, 11712 Tallinn, Estonia
Telephone: +372 521 0955, fax: +372 620 4051, e-mail: dmitri.sokolov@mail.ee

Abstract

During the last years the development of e-banking in Estonia has been very significant. According to the report of the World Economic Forum, the Estonian IT-development has been substantial. The success of e-banking in Estonia can be compared to the corresponding success of the Nordic countries. According to the Deutsche Bank Research, around 70-80% of the Internet users in Estonia use Internet banking and in this respect, Estonia could be compared to Finland, Norway and Iceland.

Despite of certain benefits, e-banking has turned out a great risk, as bank clients are expecting e-banking services to be available 24 hours a day and seven days a week. The major risks associated with e-banking are strategic, operational, legal and reputational. Security is considered the central operational risk of e-banking. Some of the specific problems cut across risk categories, e.g. breach of security allowing unauthorised access to customer information can be classified as an operational risk, but such an event also exposes the bank to legal risk and reputational risk.

Customer education on security risks and precautions can play an important role for consumer protection and for limiting reputational risk. In Estonia, all commercial banks which are engaged in e-banking activities have published on their websites recommendations to potential customers on how to increase the security while making transactions in electronic environment. The Estonian Financial Supervision Authority responsible for the banking supervision has disseminated on its website a special brochure to e-banking customers on how to use the Internet bank safely.

At the international level the Basel Committee on Banking Supervision (BCBS) has elaborated risk management principles for e-banking. These risk management principles fall into three broad, and often overlapping, categories: Board and Management Oversight, Security Controls and Legal and Reputational Risk Management. The research question of this paper is whether these risk management principles are implemented at the Estonian banks. In order to assess the risk management practices of the Estonian banks in the field of e-banking as well as their conformity to the BCBS guidelines, the author has prepared a questionnaire and circulated it to all banks. According to the results of the survey, the Estonian banks generally comply with all BCBS guidelines in the field of e-banking risk management.

JEL Classification numbers: G21

Keywords: e-banking, risks, risk management
1. Introduction

During the last years the development of e-banking in Estonia has been very significant. More and more commercial banks have realised the advantages of e-banking and therefore started to transfer their payment systems into electronic channels. According to the report of the World Economic Forum, the Estonian IT-development has been substantial (Changgyu 2003). First, from the viewpoint of practical availability of e-services, Estonia is on the eighth place among 82 countries using Internet. Second, Estonia is on the second place in the development of e-banking. And finally, Estonia is on the third place in e-government activities. The success of Estonian e-banking could be compared to the corresponding success of the Nordic countries.

40% of the Estonian population is using e-banking, which is the highest rank among 10 Central and Eastern European Countries (CEEC). The CEEC’s average was 4%; the lowest grade was in Bulgaria where according to this survey only 0.2% of the population used e-banking services. 72% of Estonian enterprises with Internet access used the Internet for banking or financial services (Danish Management 2004). The high level of e-banking in Estonian enterprises points to a high level of trust in banking services. Deutsche Bank Research (2006) has shown that around 70-80% of the Internet users in Estonia use Internet banking and in this respect, Estonia could be compared to Finland, Norway and Iceland.

The Bank for International Settlements (BIS) survey indicated that the main reasons for the popularity of e-banking in Estonia are its convenience and low cost compared to other services offered by banks (BIS 2004). According to the Wall Street Journal (Ülevaade…2000), in addition to the lower price of transactions via e-channels compared to those at bank branches, a rapid development of e-banking in Estonia can be explained by some impact of the Scandinavian information and communication technology culture on the Estonian development.

Despite of certain benefits (e.g. convenience, lower transaction costs compared to the traditional banking channels etc.), e-banking has turned out a great risk, as bank clients are expecting e-banking services to be available 24 hours a day and seven days a week. The availability of e-banking services has become extremely important during the last years: bank clients are not used to wait in electronic environment. Many e-banking risks are in fact very closely interconnected. For example, unauthorized access to the bank client’s private information causes first of all operational risk, but indirectly also legal (as client could complain to the corresponding state institutions) as well as reputational risk (client could block all accounts and discard all other banking products and services in this bank).

The paper proceeds as follows. In the second chapter the author identifies the key risks associated with e-banking. In the third chapter the author gives an overview of the international guidelines in the field of e-banking risk management as well as presents the design of the questionnaire on e-banking risk management practices of the Estonian banks. In the fourth, fifth and sixth chapters the results of the survey are presented on how risk management principles are applied by the Estonian banks in three categories: board and management oversight, security controls, and legal and reputational risk management. The seventh chapter concludes.
2. Identifying Key E-Banking Risks

Although the adoption of electronic finance and other e-services offers emerging economies an opportunity to leapfrog, it also carries potential risks. Most of the crimes that exploit the vulnerabilities inherent in these technologies are not new – fraud, theft, impersonation, denial of service and related extortion demands have plagued the financial services industry for years. However, the widespread use of these technologies exposes users to crimes of greater dimensions in terms of depth and scope (Glaessner 2003).

Strategic risk is one of the most significant risks that e-banking activities present for banking organisations. Strategic risk differs from other risk categories in that it is more general and broad in nature. Strategic decisions to be taken by a bank’s senior management have implications for all other risk categories. Given growing customer acceptance and demand for e-banking, most banks will need to develop a strategy to use the Internet delivery channel to provide informational content and/or transactional service to customers. 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 (Basel Committee 1998). Spurred by competitive and peer pressures, banks may seek to introduce or expand e-banking without an adequate cost-benefit analysis. The organizational structure and resources may not have the skills to manage e-banking. Banks should respond to strategic risk 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.

E-banking involves several specific operational risks (Schilder 2001). One operational risk mainly relates to the security of systems and transactions, including data confidentiality and authentication of the parties involved. Another operational risk refers to the continuous availability of the Internet as a medium for financial transactions. To take full advantage of the potential benefits of e-banking services, systems should be available on a 24-hour basis. This availability is prone to serious hazards, such as computer viruses and hackers. Operational risk results from reliance on complex technology. Such risks can arise not only when technology is developed in-house but also when it is outsourced. The existence of increasingly complex arrangements between a financial institution and a chain of service providers creates novel oversight problems. A significant number of banks offering e-banking services outsource related business functions, e.g. security, either for reasons of cost reduction or, as is 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.

One of the components of operational risk is the forecasts of the potential customers’ volume which in the case of e-channels have proved difficult (Sergeant 2000). Many banks going online 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 online to deal with the capacity problems.

There is also a risk which arises from legal and regulatory uncertainty in e-finance transactions referring in particular to the difficulty of identifying the
headquarters of an e-finance firm. This is the risk to earnings or capital arising from violations of, or non-conformance with, laws, regulations and ethical standards. This risk is amplified when the customer, the bank and the transaction are in more than one country. Banks engaging in e-banking can face legal risks with respect to customer disclosures and privacy protection. Customers who have not been adequately informed about their rights and obligations may bring suit against a bank. Failure to provide adequate privacy protection may also subject a bank to regulatory sanctions in some countries (Basel Committee 1998). Banks choosing to enhance customer service by linking their Internet sites to other sites also can face legal risks. A hacker may use the linked site to defraud a bank customer, and the bank could face litigation from the customer.

Because financial institutions use similar software programme, there is a systemic risk that many large institutions could be simultaneously subject to a common adverse shock. Moreover, the deeper involvement of greater numbers of new and different firms – including non-financial firms – in financial markets may make it much more difficult to monitor the links between the various actors and to assess the risks to which they are exposed. As the links between financial and non-financial markets become more pervasive, the sources of systemic risk are likely to become harder to identify (Crocket 2001).

Security is considered the central operational risk of e-banking. Threats can come from inside and outside the system. They include unauthorized access to the system through, for example, back doors, brute force, hijacking, sniffing or spoofing to retrieve and use confidential consumer information, add customer assets, subtract customer liabilities or interrupt operations. Similarly, denial of service attacks and injecting a virus can disrupt services and affect integrity of information (Schaechter 2002). Security breaches essentially fall into three categories: breaches with serious criminal intent (e.g. fraud, theft of commercially sensitive or financial information), breaches by casual hackers (e.g. defacement of web sites or denial of service – causing web sites to crash) and flaws in systems design and/or set up leading to security breaches (e.g. genuine users seeing / being able to transact on other users’ accounts). All of these threats have potentially serious financial, legal and reputational implications (Sergeant 2000).

According to the Deutsche Bank Research (2006), security concerns are the most important hurdle for many customers (see Figure 1). Cheaper fees and the possibility to ask questions are not so essential compared to the expected level of security in e-banking.

E-banking, in particular Internet banking can potentially be misused for money laundering because of the lack of face-to-face contact with customers (Schaechter 2002). Money laundering has been greatly facilitated by electronic banking because of the anonymity it affords: once a customer opens an account, it is impossible for banks to identify whether the nominal account holder is conducting a transaction or even where the transaction is taking place.

Reputational risk is considerably heightened for banks using the Internet. The Internet allows for the rapid dissemination of information, which means that any incident, either good or bad, is common knowledge within a short space of time. Internet rumours can easily become self-fulfilling prophecies. The speed of the Internet considerably cuts the optimal response times for both banks and regulators to any incident. Banks must ensure their crisis management processes are able to cope with Internet related incidents (Sergeant 2000).
Reputational risk may arise when systems or products do not work as expected and cause widespread negative public reaction. A significant breach of security, whether as a result of external or internal attacks on a bank’s system, can undermine public confidence in a bank. Reputational risk may also arise in cases where customers experience problems with a service, but have not been given adequate information about product use and problem resolution procedures. Mistakes, malfeasance, and fraud by third parties may also expose a bank to reputational risk. Reputational risk can arise from significant problems with communications networks that impair customers’ access to their funds or account information, particularly if there are no alternative means of account access. Substantial losses caused by mistakes of another institution offering the same or similar electronic banking products or service may cause a bank’s customers to view its products or service with suspicion, even if the bank itself did not face the same problems. Reputational risk may also arise from targeted attacks on a bank. For example, a hacker penetrating a bank’s web site may alter it to intentionally spread inaccurate information about the bank or its products. Reputational risk may not only be significant for a single bank but also for the banking system as a whole. If a globally active bank experienced important reputational damage concerning its electronic banking business, the security of other banks’ systems may also be called into question. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system as a whole (Basel Committee 1998).

Customer education on security risks and precautions can play an important role for consumer protection and for limiting reputational risk. Security risks can be heightened when a consumer does not understand the necessary security precautions and misuses them inadvertently. Banks should therefore provide prominent and easy-to-understand advice to customers on the importance of security precautions and concerning personal privacy policies. This guidance should be understood before any e-banking services are activated (Schaechter 2002). For supervisors, assisting in the educational process and requiring banks to raise consumer awareness can become a key means to help protect consumers. A number of supervisory authorities view education
as part of their mandate to consumer protection and have increased their efforts in that respect.

Regarding the situation in Estonia, all commercial banks which are engaged in e-banking activities have published on their websites recommendations to potential customers on how to increase the security while making transactions in electronic environment. In addition, banks have provided all necessary contact details of customer support service. The Estonian Financial Supervision Authority responsible for the banking supervision has disseminated on its website a special brochure to e-banking customers on how to use the Internet bank safely. This booklet contains important information on user’s ID and passwords, how to ensure the security of personal computers, how to enter and leave the Internet bank, as well as how to block an Internet bank service.

3. Designing the Questionnaire on E-Banking Risk Management Practices

At the international level the issues of e-banking and its risk management have become very topical. According to the Basel Committee on Banking Supervision (BCBS), the rapid development of e-banking carries benefits as well as risks and BCBS expects such risks to be recognised, addressed and managed by banking institutions in a prudent manner (Basel Committee 2003). These developments led the BCBS to conduct a preliminary study of the risk management implications of e-banking and e-money in 1998. This early study demonstrated a clear need for more work in the area of e-banking risk management and that mission was entrusted to a working group comprised of bank supervisors and central banks, the Electronic Banking Group (EBG), which was formed in November 1999. The BCBS released the EBG’s Report on risk management and supervisory issues arising from e-banking developments in October 2000. The EBG concluded that e-banking activities did not raise risks that were not already identified by previous work of the BCBS. However, it noted that e-banking increases and modifies some of these traditional risks, thereby influencing the overall risk profile of banking. In particular, strategic risk, operational risk and reputational risk are certainly heightened by the rapid introduction and underlying technological complexity of e-banking activities.

In 2003, BCBS identified fourteen risk management principles for electronic banking to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities. These risk management principles fall into three broad, and often overlapping, categories: Board and Management Oversight, Security Controls and Legal and Reputational Risk Management (Basel Committee 2003).

In order to assess the risk management practices of the Estonian banks in the field of e-banking as well as their conformity to the BCBS guidelines, the author has prepared a questionnaire on the basis of the risk management principles identified by the BCBS and circulated it to all banks and branches of foreign credit institutions (hereinafter banks) operating in Estonia. It should be noted that there are 14 banks in Estonia in total, but as two banks are not involved in e-banking at all, the questionnaire was sent to 12 banks. The following banks participated in the survey: Hansapank, SEB Eesti Ühispank, Sampo Pank, Nordea Pank, Eesti Krediidipank, SMB Pank, Tallinna Äripank, Balti Investeeringute Grupi Pank, DnB NORD Pank, Parex Pank, Handelsbanken and Bayerische Hypo- und Vereinsbank (currently UniCredit). The
questions were addressed mainly to the banks’ risk managers or e-banking specialists residing either in Estonia or abroad in the case of several branches of foreign credit institutions.

The BCBS risk management principles are not put forth as absolute requirements or even best practice. The BCBS believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated because of the speed of change related to technological and customer service innovation (Basel Committee 2003). As the BCBS has not elaborated detailed criteria for assessing how one or another risk management technique works in reality, the author has constructed the questionnaire using the dichotomous scale of answers where the bank’s risk manager or specialist could choose either Yes or No response.

As right from the beginning the questionnaire was circulated to the persons directly involved in e-banking issues without any intermediate and also taking into account that the author conducted several follow-ups by telephone and e-mail, the response rate in this survey was really excellent. All 12 banks responded to the e-banking risk management questionnaire, e.g. the response rate was 100%. Consequently, the further analysis of banks’ responses would make it possible to make conclusions regarding the whole Estonian banking market’s developments.

4. Board and Management Oversight of E-Banking Risks at the Estonian Banks

Because the Board of Directors and senior management are responsible for developing the institution’s business strategy and establishing an effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context (Basel Committee 2003). In Ramakrishnan’s view (2001), managing the risks and implementing controls for e-banking initiatives follows the same principles as other risk management processes. The most dangerous thing is to treat this as a technical problem and leave it to IT management to manage – this is a general management issue, which needs attention from senior management.

Practically all banks in Estonia have established an effective management oversight over the risks associated with e-banking which includes the implementation of specific accountability, policies and controls to manage these risks. The reason why one bank has not done so is that transactional e-banking is not a priority for that bank and currently it is not involved in transactional e-banking operations at all (see Figure 2).

In line with the best risk management practices, bank’s risk managers should not belong to the business units dealing with e-banking products’ and services’ development and sale. Taking this into account, the author included a question regarding the independence of the employees responsible for e-banking risk management from the business units.
Figure 2. The Establishment of Management Oversight of E-Banking Risks at the Estonian Banks

- Yes, an effective management oversight over the risks associated with e-banking has been established by the senior management of the Bank: 92%
- No: 8%

Source: author’s survey

In six banks the senior management has assured the full independence of e-banking risk managers from the business units (see Figure 3). Other 50% of the banks answered that e-banking risk managers are not independent from the business units, e.g. the position of the bank’s employee responsible for e-banking risk management belongs to the business unit rather than to the risk management department or these two functions could be linked at the bank.

Figure 3. The Position of E-Banking Risk Managers at the Estonian Banks

- Yes, the senior management has assured the full independence of the employees responsible for e-banking risk management from the business unit(s): 50%
- No: 50%

Source: author’s survey
The bank’s senior management should ensure that its risk management processes for e-banking activities are integrated into the bank’s overall risk management approach. As e-banking carries various traditional banking risks, it is important that the bank’s senior management would evaluate the existing risk management practices to ensure they are robust enough to cover the new risks posed by current or planned e-banking activities. In addition, as it was stated before, it is dangerous to treat e-banking as a technical issue and leave the establishment of e-banking risk management only to e.g. IT management.

Figure 4. The Inclusion of E-Banking Risk Management Process into the Bank’s Overall Risk Management Approach

From the banks’ answers to the e-banking risk management questionnaire it could be noticed that in the majority of banks – 83% – the process of e-banking risk management has been integrated into the bank’s overall risk management approach by the approval of the senior management (see Figure 4). In two banks, however, e-banking risk management process exists as a separate risk management field.

Bank’s senior management should ensure that the operational and security risk dimensions of the institution’s e-banking business strategies are appropriately considered and addressed. Consequently, according to the Basel Committee (2003), effective management oversight is expected to encompass the review and approval of the key aspects of the bank’s security control process, such as development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats.

83% of the banks responded that the senior management has reviewed and approved the key aspects of the bank’s security control process which safeguards e-banking systems and data from both external and internal threats (see Figure 5). 17% of banks responded negatively, e.g. there is no formal approval by the senior management of the security control process associated with e-banking area.
Figure 5. The Establishment of a Comprehensive Security Control Process at the Estonian Banks

- Yes, the senior management has reviewed and approved the key aspects of the Bank's security control process which safeguards e-banking systems and data from both internal and external threats (17%)
- No (83%)

Source: author’s survey

Effective management oversight should also include a comprehensive process for managing risks associated with increased complexity of outsourcing relationships and third-party dependencies to perform critical e-banking functions (Basel Committee 2003). Increased reliance upon partners and third party service providers to perform critical e-banking functions lessens the bank management’s direct control. Accordingly, a comprehensive process for managing the risks associated with outsourcing and other third-party dependencies is necessary.

Figure 6. The Existence of Management Oversight Process for Outsourcing at the Estonian Banks

- Yes, the senior management has established a comprehensive and ongoing oversight process for managing the Bank's outsourcing relationships and other third-party dependencies (33%)
- No (67%)
2/3 of the Estonian banks responded that at their bank the senior management has established a comprehensive and ongoing due diligence and oversight process for managing the bank’s outsourcing relationships and other third-party dependencies (see Figure 6). 1/3 of the banks who responded to this question negatively mentioned that the main reason was that until now all e-banking products have been developed by banks themselves and not outsourced from other parties. That is why there is no need to establish an outsourcing oversight process at the management level, at least at the present stage.

5. Security Control Processes for E-Banking at the Estonian Banks

While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking. This should include establishing appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities and data integrity of transactions, records and information. In addition, the existence of clear audit trails for all e-banking transactions should be ensured and measures to preserve confidentiality of key e-banking information should be appropriate with the sensitivity of such information (Basel Committee 2003).

It is essential in banking to confirm that a particular communication, transaction or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions (Basel Committee 2003). Failure on the part of the bank to adequately authenticate customers could result in unauthorised individuals gaining access to e-banking accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activity.

In the sixth question of the questionnaire on e-banking risk management the author asked the banks whether they had established appropriate measures to authenticate the identity and authorisation of e-banking customers. The results obtained via the questionnaire have shown that all banks in Estonia have established the corresponding measures, e.g. the identity and authorisation of the Estonian banks’ existing and potential e-banking customers is properly authenticated.

The next EBG principle for e-banking risk management states that banks should use transaction authentication methods that promote non-repudiation and

---

1 Authentication is the techniques, procedures and processes used to verify the identity and authorisation of e-banking customers
Identification is the procedures, techniques and processes used to establish the identity of a customer
Authorisation is the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the bank account or the authority to conduct associated transactions on that account
2 Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message
establish accountability for e-banking transactions (Basel Committee 2003). Non-repudiation involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data have been received or to protect the recipient against false denial by the sender that the data have been sent. Risk of transaction repudiation is already an issue with conventional transactions such as credit cards or securities transactions. However, e-banking heightens this risk because of the difficulties of positively authenticating the identities and authority of parties initiating transactions, the potential for altering or hijacking electronic transactions, and the potential for e-banking users to claim that transactions were fraudulently altered.

In the case of Estonia, all banks have implemented e-banking transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions according to the results of e-banking risk management survey, e.g. the Estonian e-banking client is protected against false denial by the bank that the banking data have been received and, at the same time, the bank is protected against false denial by its e-banking customer that the data have been sent.

Segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems and to ensure that transactions and company assets are properly authorised, recorded and safeguarded. Segregation of duties is critical to ensuring the accuracy and integrity of data and is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud can only be committed through collusion (Basel Committee 2003). E-banking services may necessitate modifying the ways in which segregation of duties are established and maintained because transactions take place over electronic systems where identities can be more readily masked or faked. In addition, operational and transaction-based functions have in many cases become more compressed and integrated in e-banking applications. Therefore, the controls traditionally required to maintain segregation of duties need to be reviewed and adapted to ensure an appropriate level of control is maintained.

According to the results of the questionnaire, all Estonian banks have established appropriate measures to promote an adequate segregation of duties within e-banking systems, databases and applications, e.g. the risk of fraud in bank’s operational systems and processes has been reduced by the banks.

In order to maintain segregation of duties, banks need to strictly control authorisation and access privileges. According to the Basel Committee (2003), failure to provide adequate authorisation control could allow individuals to alter their authority, circumvent segregation and gain access to e-banking systems, databases or applications to which they are not privileged. In the Estonian e-banking specialists’ opinion, all banks have applied proper authorisation controls and access privileges in e-banking systems, databases and applications.

Failure to maintain the data integrity\(^3\) of transactions, records and information can expose banks to financial losses as well as to substantial legal and reputational risk (Basel Committee 2003). In Estonia, according to the results of e-banking risk management survey conducted by the author, all banks have applied appropriate measures to protect the data integrity of e-banking transactions, records and

\(^3\) Data integrity is the state of data in case destructions, undesirable changes and losses are missing

32
information, e.g. it is not possible to modify the banking information within e-banking systems without proper authorisation.

Delivery of financial services over the Internet can make it more difficult for the banks to apply and enforce internal controls and maintain clear audit trails if these measures are not adapted to an e-banking environment. Banks are not only challenged to ensure that effective internal control can be provided in highly automated environments, but also that the controls can be independently audited, particularly for all critical e-banking events and applications. A bank’s internal control environment may be weakened if it is unable to maintain clear audit trails for its e-banking activities (Basel Committee 2003). This is because much, if not all, of its records and evidence supporting e-banking transactions are in an electronic format.

In their responses to the e-banking risk management questionnaire all banks stated that clear audit trails had been implemented for all e-banking transactions, e.g. the Estonian banks keep records on the persons who have had an access to the e-banking systems and what operations have been performed there during a certain time.

Confidentiality is the assurance that key information remains private to the bank and is not viewed or used by those unauthorised to do so. Misuse or unauthorised disclosure of data exposes a bank to both reputational and legal risk. The advent of e-banking presents additional security challenges for banks because it increases the exposure that information transmitted over the public network or stored in databases may be accessible by unauthorised or inappropriate parties or used in ways the customer providing the information did not intend (Basel Committee 2003). Additionally, increased use of service providers may expose key bank data to other parties.

In Estonia, according to the banks’ responses to the questionnaire, all banks have applied measures which are commensurate with the sensitivity of the information being transmitted and/or stored in databases in order to preserve the confidentiality of key e-banking information, e.g. information transmitted via e-banking channels is not accessed or used by the unauthorised persons.

6. Legal and Reputational Risk Management at the Estonian Banks

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they can expect when using traditional banking distribution channels.

To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, banks should ensure that adequate information is provided on their websites to allow customers make informed conclusions about the identity and regulatory status of the bank before they enter into e-banking transactions (Basel Committee 2003).

According to the survey results, all banks in Estonia have ensured that prior to entering into e-banking transactions adequate information is provided on their websites to allow customers make an informed conclusion about the bank identity (e.g. contact details, customer support, information on the offered e-products’ and e-services’

\[4\] Audit trail is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time
conditions) and regulatory status, e.g. all Estonian banks provide sufficient information disclosures to their existing and potential e-banking customers.

Maintaining a customer’s information privacy is a key responsibility for a bank. Misuse or unauthorised disclosure of confidential customer data exposes a bank to both legal and reputational risk. To meet these challenges, banks should make reasonable endeavours to ensure that the bank’s customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-banking products and services (Basel Committee 2003). According to the banks’ responses to the e-banking risk management questionnaire, all banks in Estonia have applied appropriate measures to ensure adherence to customer privacy requirements.

To protect banks against business, legal and reputational risk, e-banking services must be delivered on a consistent and timely basis in accordance with customer expectations. Therefore, the bank must have the ability to deliver e-banking services to end-users from either primary (e.g. internal bank systems and applications) or secondary sources (e.g. systems and applications of service providers). The maintenance of adequate availability is also dependent upon the ability of contingency back-up systems to mitigate denial of service attacks or other events that may potentially cause business disruption. The challenge to maintain continued availability of e-banking systems and applications can be considerable given the potential for high transaction demand, especially during peak time periods. In addition, high customer expectations regarding short transaction processing cycle times and constant availability (24 hours a day and seven days a week) has also increased the importance of sound capacity, business continuity and contingency planning (Basel Committee 2003).

Figure 7. The Existence of Capacity, Business Continuity and Contingency Planning at the Estonian Banks

![Pie chart showing 83% Yes, the Bank has effective business continuity planning processes to help ensure the continuous availability of e-banking systems and services, and 17% No. Source: author’s survey](image-url)
To protect banks against business, legal and reputational risk, e-banking services must be delivered on a consistent and timely basis in accordance with customer expectations. Therefore, the bank must have the ability to deliver e-banking services to end-users from either primary (e.g. internal bank systems and applications) or secondary sources (e.g. systems and applications of service providers). The maintenance of adequate availability is also dependent upon the ability of contingency back-up systems to mitigate denial of service attacks or other events that may potentially cause business disruption. The challenge to maintain continued availability of e-banking systems and applications can be considerable given the potential for high transaction demand, especially during peak time periods. In addition, high customer expectations regarding short transaction processing cycle times and constant availability (24 hours a day and seven days a week) has also increased the importance of sound capacity, business continuity and contingency planning (Basel Committee 2003).

In Estonia, 83% of the banks have established effective capacity, business continuity and contingency planning processes to help ensure the continuous availability of e-banking systems and services (see Figure 7). Only two banks do not have operational business continuity planning processes whereby one bank is currently making active preparations to establish them.

Effective incident response mechanisms are critical to minimise operational, legal and reputational risks arising from unexpected events such as internal and external attacks that may affect the provision of e-banking systems and services. Banks should develop appropriate incident response plans, including communication strategies that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services including those originating from outsourced systems and operations (Basel Committee 2003).

The results of the survey on e-banking risk management have shown that all Estonian banks have developed appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks that may hamper the provision of e-banking systems and services.

7. Conclusions

The key risks associated with the field of e-banking are strategic, operational, reputational and legal. Some of the specific problems cut across risk categories, e.g. a breach of security allowing unauthorised access to customer information, can be classified as an operational risk, but such an event also exposes the bank to legal risk and reputational risk.

Security is considered the central operational risk of e-banking. According to the Deutsche Bank Research, security concerns are the most important hurdle for many e-banking customers. Cheaper fees and the possibility to ask questions in electronic environment are not so essential compared to the expected level of security.

Customer education on security risks and precautions can play an important role for consumer protection and for limiting reputational risk. For supervisors, assisting in the educational process and requiring banks to raise consumer awareness can become a key means to help protect consumers.

In Estonia, all commercial banks which are engaged in e-banking activities have published on their websites recommendations to potential customers on how to increase the security while making transactions in electronic environment. In addition, banks have provided all the necessary contact details of customer support service. The
Estonian Financial Supervision Authority responsible for the banking supervision has disseminated on its website a special brochure to e-banking customers on how to use the Internet bank safely. This booklet contains important information on user’s ID and passwords, how to ensure the security of personal computers, how to enter and leave the Internet bank as well as how to block an Internet bank service.

At the international level the issues of e-banking and its risk management have become very topical. According to the Basel Committee on Banking Supervision (BCBS), e-banking increases and modifies some of the traditional banking risks, thereby influencing the overall risk profile of banking. In particular, strategic risk, operational risk and reputational risk are certainly heightened by the rapid introduction and underlying technological complexity of e-banking activities. In 2003, the BCBS identified fourteen risk management principles for electronic banking to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities. These risk management principles fall into three broad, and often overlapping, categories: Board and Management Oversight, Security Controls and Legal and Reputational Risk Management.

In order to assess the risk management practices of the Estonian banks in the field of e-banking as well as their conformity to the BCBS guidelines, the author has prepared a questionnaire and circulated it to all banks and branches of foreign credit institutions operating in Estonia. As two banks are not involved in e-banking at all, the questionnaire was sent to twelve banks. The questions were addressed mainly to the banks’ risk managers or e-banking specialists residing either in Estonia or abroad in the case of several branches of foreign credit institutions. As the BCBS has not elaborated detailed criteria for assessing how one or another risk management technique works in reality, the author has constructed the questionnaire using the dichotomous scale of answers. The bank’s risk manager or specialist could choose either Yes or No response while assessing whether the concrete risk management principle has been applied by the bank or not.

As right from the beginning the questionnaire was circulated to the persons directly involved in e-banking issues without any intermediate and also taking into account that the author conducted several follow-ups by telephone and e-mail, the response rate in this survey was excellent. All twelve banks have responded to the e-banking risk management questionnaire, e.g. the response rate was 100%. Consequently, on the basis of the answers received it was possible to make conclusions regarding the whole Estonian banking market’s developments in the field of e-banking risk management.

As far as board and management oversight of e-banking risks is concerned, practically all banks have applied in their internal risk management the BCBS guidelines. However, in the case of two banks there was no formal confirmation at the level of bank’s senior management of the security control process over e-banking area. In addition, in six banks (50% of responses) e-banking risk managers are not independent from the business units, e.g. the position of the bank’s employee responsible for e-banking risk management belongs to the business unit rather than to the risk management department or these two functions could be linked at the bank. In two banks, e-banking risk management process exists as a separate risk management field and has not been integrated into the bank’s overall risk management approach.

As the major concern for e-banking customers is the security of e-channels, it is essential that banks would have appropriate security control processes for e-banking.
The results of e-banking risk management survey have shown that the Estonian banks fully comply with the BCBS risk management principles in this respect.

In the field of legal and reputational risk management the banks generally conform to the BCBS guidelines. High customer expectations regarding short transaction processing cycle times and constant availability (24 hours a day and seven days a week) of e-banking channels have increased the importance of sound capacity, business continuity and contingency planning. The results of the survey have shown that only two banks in Estonia do not have operational business continuity planning processes whereby one bank is currently making active preparations to establish them.

References