E-Banking in Estonia: Regional Development and Risk Management Practices

Dmitri Sokolov
PhD Student
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 electronic banking (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. The success of e-banking in Estonia could be compared to the corresponding success of the Nordic countries. There are five regions in Estonia and no research has been conducted so far on the regional development of e-banking. The first research question in the paper is whether e-banking is uniformly spread around the whole territory of Estonia or it is concentrated mainly in the capital city Tallinn and the Harju county. In order to assess the regional development of e-banking in Estonia, the author conducted a special survey among all banks which made it possible to assess the usage of different payment instruments at the Estonian regions. The results of the survey have shown that the distribution of e-banking channels which consist of card payments via ATM or at POS, direct debit, standing order, telebank, telephone bank, Internet bank and mobile phone payments is quite uniform in all five regions constituting 94%-97% of all payments. At the same time, the share of payments via bank branches during the last three years (2004-2006) has declined in all regions.

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 operational, legal and reputational. 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 second research question 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 the second questionnaire and circulated it to all banks. According to the results of the second 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, regional development, 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.

Modern history of the Estonian banking industry goes back into the year 1988 when permission for the establishment of commercial banks was granted for the first

time in the former Soviet Union. Estonia can boast the very first Internet banking products in Eastern Europe. Eesti Forekspank opened its Forex Direct in May 1996 and Eesti Hoiupank was quick to follow with its Panganet. In January 1998, the banks raised the service fees for cash transactions in order to popularise the non-cash payment system through telephone, Internet and telebanking (Estonian Banking Association 2003).

40% of the Estonian population is using e-banking, which is the highest rank between 10 Central and Eastern European Countries (CEEC). The CEEC's average rank 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.

The Bank for International Settlements (BIS) survey indicated that the main reasons for the popularity of Internet 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 could 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. The previous research has shown that the major risks associated with e-banking are operational, legal and reputational. 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 presents the design of the questionnaire on the regional distribution of different payment instruments in Estonia as well as analyses the results and makes international comparisons. The third chapter gives an overview of the major risks associated with e-banking. In the fourth chapter the author discusses the international guidelines in the field of e-banking risk management and the design of the second survey on e-banking risk management practices of the Estonian banks. In the fifth, sixth and seventh chapters the author presents the results of the second survey 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 eighth chapter concludes.

2. Regional Development of E-Banking in Estonia

According to the Eesti Pank (Bank of Estonia) Governor's Decree No. 9 of 9 October 2003, the Bank of Estonia collects payment statistics from the credit institutions licensed in Estonia and branches of foreign credit institutions (hereinafter *banks*). Banks are obliged to submit the report on payments and the report on card

transactions and mobile phone payments on a monthly basis. In addition, banks submit the report on cards and the report on Automated Teller Machines (ATM) and Point of Sale (POS) on a quarterly basis. The first two monthly reports give a good overview of the distribution of different payment instruments in Estonia.

However, for the needs of the current research it would not be possible to use the reports collected by the Bank of Estonia for two reasons. First, these reports do not have a regional component, e.g. they contain the data on the whole Estonia, but not on its regional units. Second, the classification of payment instruments in these reports is somewhat different – e.g. it is not possible to identify the payments made in bank branches.

Taking into account the goal to assess the regional development of e-banking in Estonia, the author decided to conduct a special survey in the form of questionnaire. Currently there are fourteen banks operating in Estonia of which eleven are obliged to submit payment reports to the Bank of Estonia. Consequently, the author contacted only these eleven banks' accountants or reporting specialists and asked them to provide the data on the number of payment instruments by three consecutive years: 2004, 2005 and 2006. The payment instruments for the needs of the future analysis in this research were classified differently from the Bank of Estonia's classification and were as follows:

1. Branch
2. Card Payments (POS, ATM)
3. Direct Debit[1]
4. Standing Order[2]
5. Telebank[3]
6. Telephone Bank
7. Internet Bank
8. Mobile Phone Payments
9. Other Payments
10.

According to the administrative division Estonia consists of 15 counties. For the purposes of the research these 15 counties were divided into 5 regions as follows:

Northern Estonia	Harju county
Western Estonia	Hiiu, Lääne, Pärnu and Saare counties
Central Estonia	Järva, Lääne-Viru and Rapla counties
North-Eastern Estonia	Ida-Viru county
Southern Estonia	Jõgeva, Põlva, Tartu, Valga, Viljandi and Võru counties

Thus, the banks were asked to fill in six tables: distribution of payment instruments during the period of 2004-2006 in the total Estonia, Northern Estonia, Western Estonia, Central Estonia, North-Eastern Estonia and Southern Estonia.

Six banks out of eleven sent the filled-in questionnaires back, thus making the response rate of 55%. By 31 December 2006 the market share of these banks by total assets constituted 26%. Taking into account the high concentration of the Estonian banking market and the certain limitations of the data collection, the author considers

[1] Debit order recurring with fixed frequency
[2] Credit order with a fixed sum of money recurring with fixed frequency
[3] Payment by means of a special software either on-line or off-line (Dial-up connection)

the response rate to be good. Also, among the banks which have responded to the questionnaire were several banks with banking activities throughout the whole Estonia. That is why in the author's opinion, it is possible to extend the results of the survey to the whole banking sector.

The major reasons why the remaining five banks were not able to provide the data were the following:

- According to the structure of the Bank of Estonia's report on payments, the data on the location of a customer (payer) is not obligatory. That is why several banks do not keep such information in the existing queries. In order to make the information on the payer's location available, a bank should make new queries which at least for some banks turned out very capacious, time-consuming and expensive task;
- The author asked banks to provide the data on a yearly basis. However, the reports submitted to the Bank of Estonia are on a monthly basis. In order to complete the questionnaire, banks should make queries from different databases by different months which could overload the system and distract bank's current works.

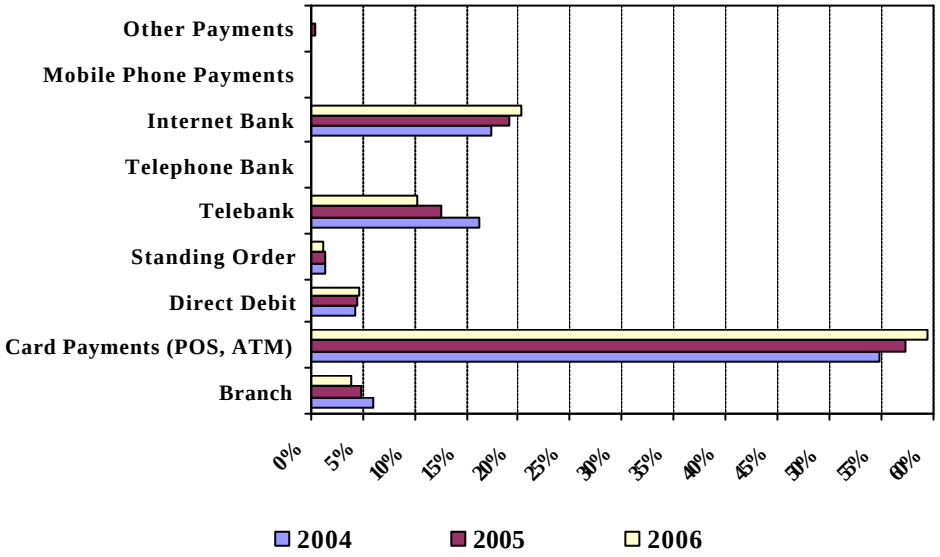

Figure 1. The Distribution of Payment Instruments in Estonia

First, if we look at the aggregated numbers regarding the usage of different payment instruments in Estonia, we could notice that the share of electronic channels during the last three years has increased. All seven payment instruments – Internet bank, card payments either via ATM or at POS, telebank, direct debit, standing order, telephone bank and mobile phone – are in fact e-banking channels and their aggregated share increased by 2 percentage points in 2006 compared to 2004, up to 96%. At the same time, the share of payments via bank branches decreased from 5.9% in 2004 to 3.8% in 2006.

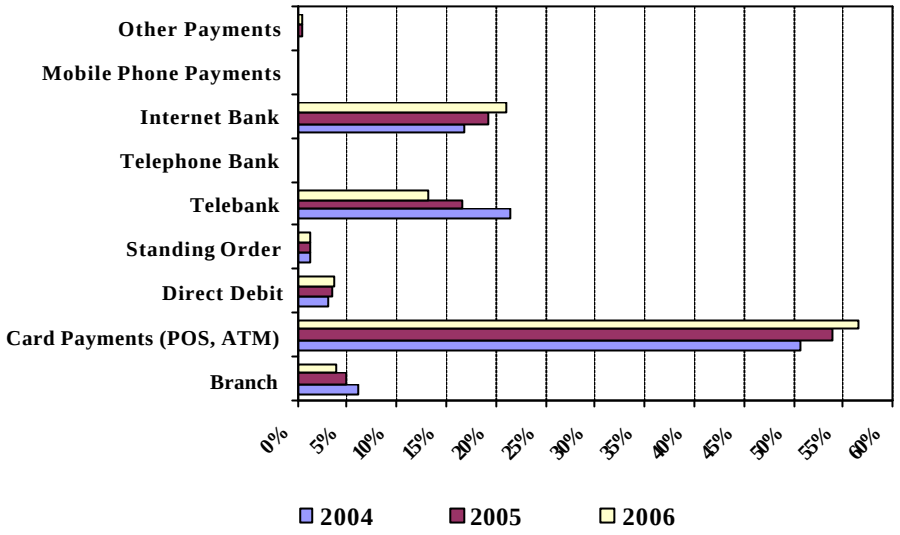

Figure 2. The Usage of Different Payment Instruments in Northern Estonia

If we analyse the data on the usage of payment instruments in Northern Estonia (to remind, this region consists of the Harju county and the capital city Tallinn), the same tendency could be discovered: the share of bank branches decreased, while the share of e-banking channels increased. The most popular payment instruments in Northern Estonia are card payments via ATM and at POS and Internet bank, in two years their shares increased by 5.6 and 4.2 percentage points respectively. The aggregated share of e-banking channels increased from 93.5% up to 95.6% in 2006.

Is the usage of e-banking channels also popular in other regions of Estonia or e-banking is concentrated mainly in the capital city Tallinn and its county Harju? The analysis of banks' responses to the questionnaire made it possible to answer this question.

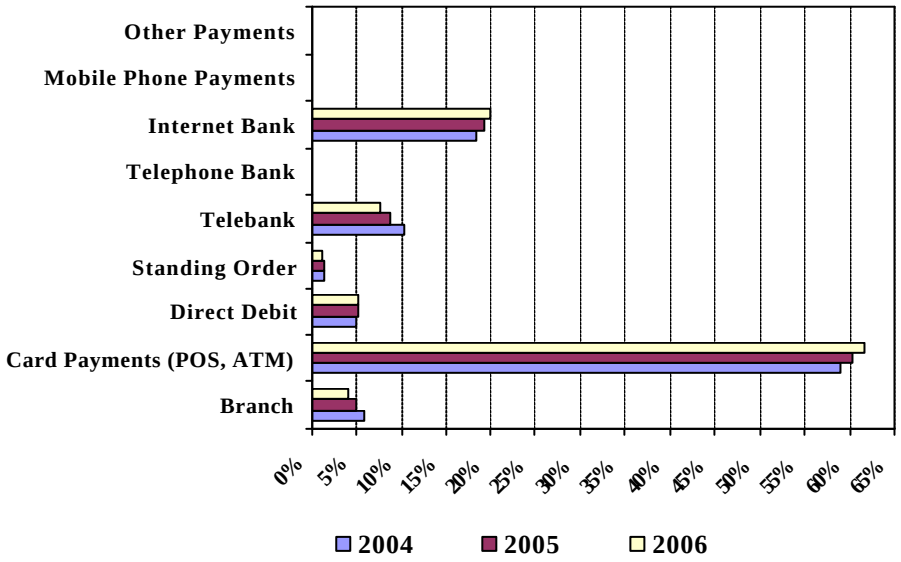

Figure 3. The Distribution of Payment Instruments in Western Estonia

In Western Estonia comprised of 4 counties (Hiiu, Lääne, Pärnu and Saare) the share of payments made via branches is also quite negligible, only 4% by the end of 2006,

having declined by around 2 percentage points compared to 2004. The usage of card payments is even more popular than in Tallinn and the Harju county constituting 62% of total payments compared to 56% in Northern Estonia.

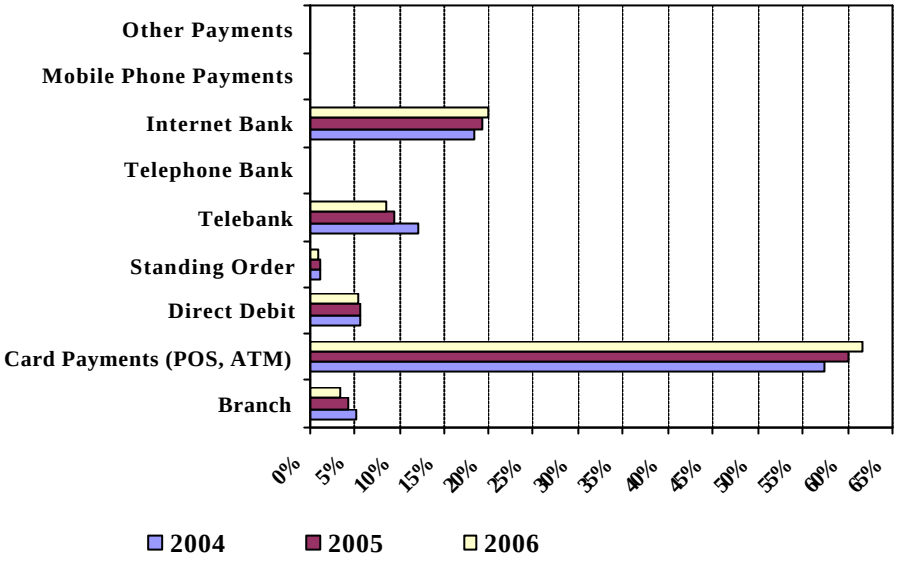

Figure 4. The Usage of Different Payment Instruments in Central Estonia

Central Estonia consists of 3 counties: Järva, Lääne-Viru and Rapla. The share of bank branches here is one of the lowest in Estonia constituting only 3.3% of all payments and decreasing within the last three years. As in other Estonian regions, the most popular payment channels are card payments in ATM and at POS as well as Internet banking. During three years the aggregated share of electronic channels has increased by around 2 percentage points, up to 96.6%.

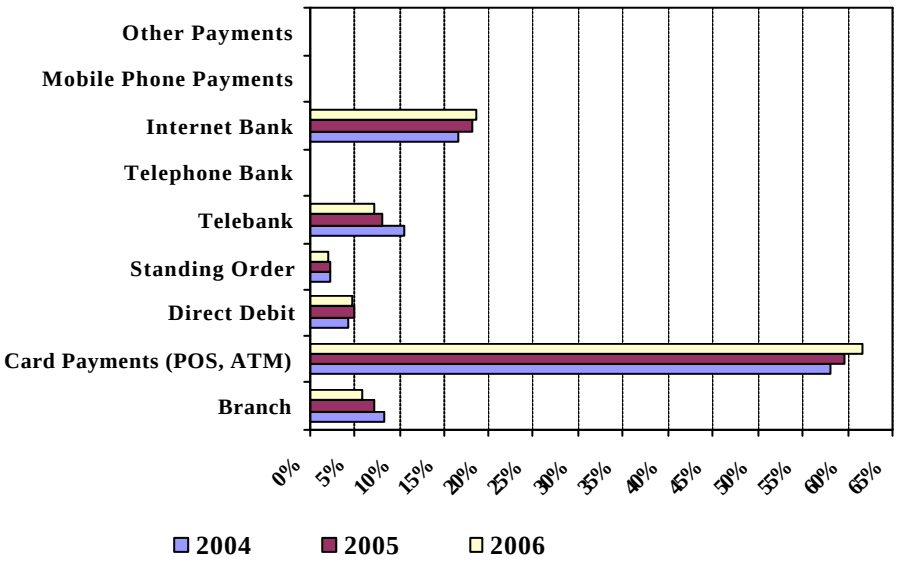

Figure 5. The Distribution of Payment Instruments in North-Eastern Estonia

If we look at the payment preferences in North-Eastern Estonia consisting of one county, Ida-Viru, we could discover that the share of payments via bank offices is the

highest here, 5.8%. However, like in the other regions, the share of branches is declining being substituted by ever increasing popularity of e-banking channels.

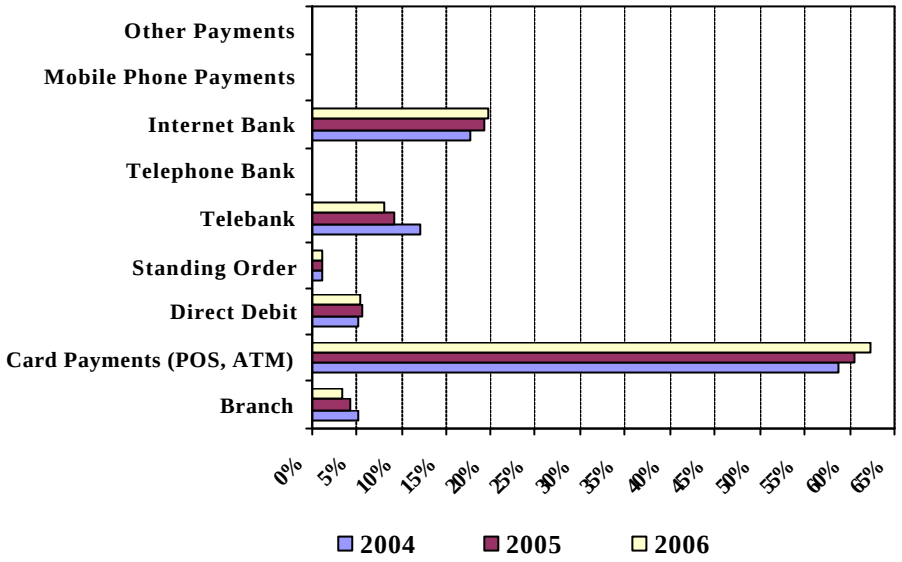

Figure 6. The Usage of Different Payment Instruments in Southern Estonia

In Southern Estonia comprised of Jõgeva, Põlva, Tartu, Valga, Viljandi and Võru counties, the share of bank branches is one of the lowest. Like in Central Estonia, it was only 3.3% of total payments at the end of 2006 and during three years their share has declined by 1.8 percentage points.

If we compare the regional distribution of payment instruments in Estonia with that in Finland, we can notice that in general the usage of e-banking in Estonia is very high like in Finland. However, in Finland, according to the Finnish Bankers' Association (2004), the share of e-banking channels is the highest at the capital region (around 93%) and the lowest in the countryside (around 83%), e.g. the significance of branch offices is quite large there compared to the capital region. In this respect, the regional distribution of payment instruments is more even in Estonia where in all regions the share of e-banking channels varies from 94% to 97%.

3. Risks of E-Banking

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).

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.

Four risk categories associated with the development of e-banking could be identified (Crocket 2001). First, there is the risk of strategic and business misjudgements. E-banking is relatively new on strategic risk and, as a result, there can be a lack of understanding among senior management about its potential and implications. Regarding business risk, taking into account the newness of e-banking, nobody knows much about whether e-banking customers will have different characteristics from the traditional banking customers.

The second risk is operational, resulting from reliance on complex technology. 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.

The third risk 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.

The fourth risk is systemic risk. Because financial institutions use similar software programs, there is a risk that many large institutions could be simultaneously subject to a common adverse shock.

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). Outsourcing is an additional security threat, which can also have a major impact on the data and system integrity and availability.

E-banking, in particular Internet banking, can potentially be misused for money laundering because of the lack of face-to-face contact with customers. 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 (Nsouli 2002).

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.

4. Studying E-Banking Risk Management Practices of the Estonian Banks

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 the 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 (Basel Committee 2003). 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 the 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 2 banks are not involved in e-banking at all, the questionnaire was sent to 12 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.

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 the 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 have 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.

5. Board and Management Oversight of E-Banking Risks in Estonia

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).

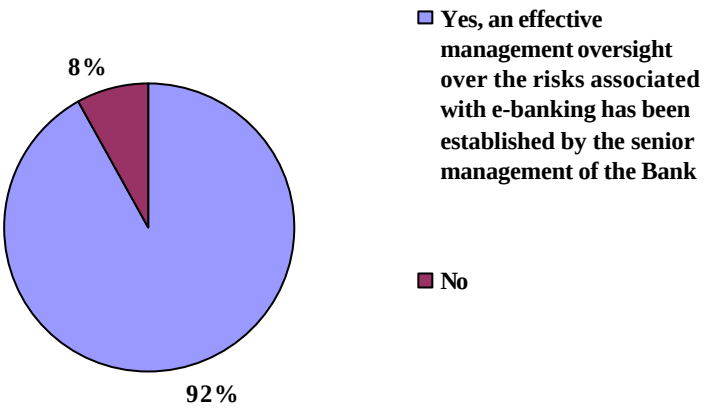

Figure 7. The Establishment of Management Oversight of E-Banking Risks at the Estonian Banks

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.

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, effective management oversight is expected to encompass the review and approval of the key aspects of the bank's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats (Basel Committee 2003).

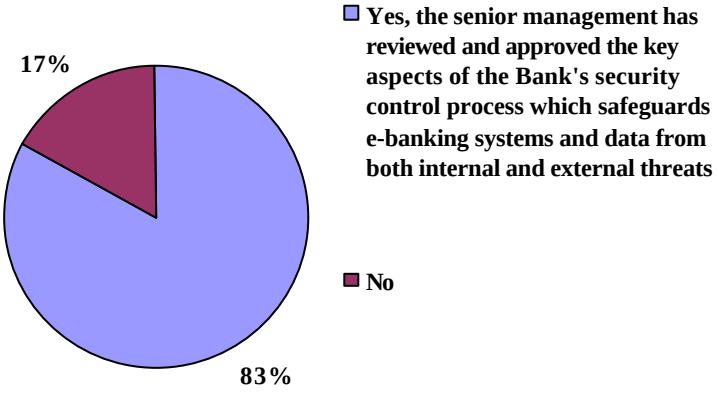

Figure 8. The Establishment of a Comprehensive Security Control Process at the Estonian Banks

83% of 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. 17% of banks responded negatively, e.g. there is no formal approval by the senior management of security control process associated with e-banking area.

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

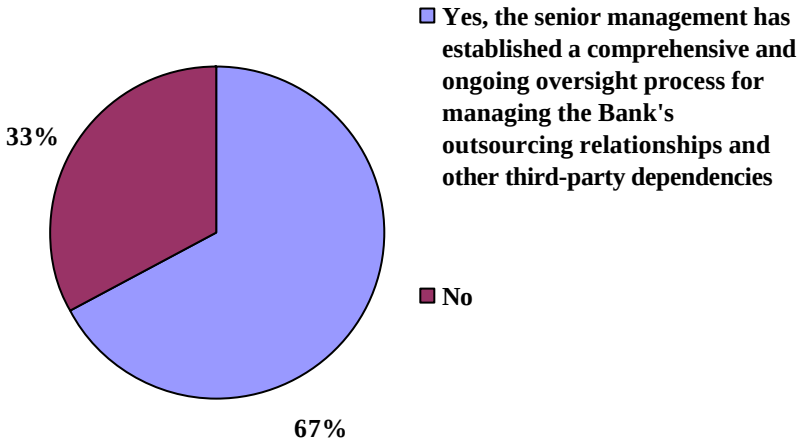

Figure 9. The Existence of Management Oversight Process for Outsourcing at the Estonian Banks

2/3 of the Estonian banks responded that at their banks 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. 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.

6. Security Control Processes for E-Banking in Estonia

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).

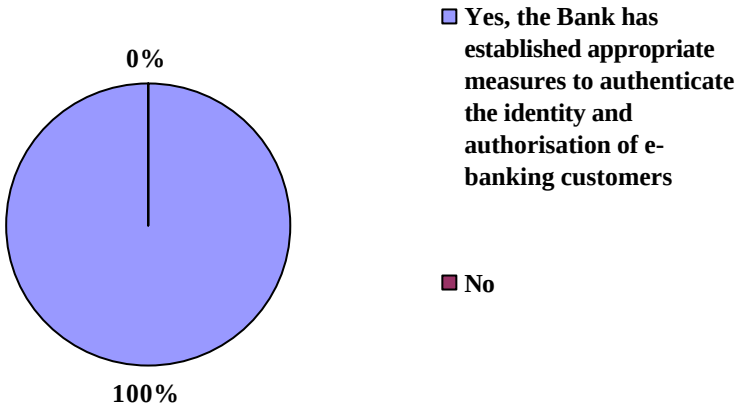

Figure 10. Authentication of E-Banking Customers at the Estonian Banks

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[4] the identity and authorisation of established customers seeking to initiate electronic transactions. 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 (Basel Committee 2003).

The analysis of the questionnaire on e-banking risk management has shown that all banks in Estonia have established appropriate measures to authenticate the identity and authorisation of e-banking customers, e.g. banks do fully conform to the BCBS guidelines in this respect.

[4] 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

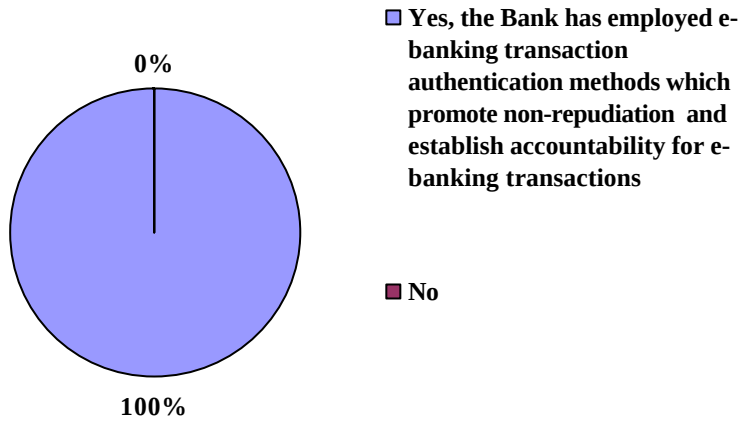

Figure 11. The Existence of Non-Repudiation and Accountability for E-Banking Transactions at the Estonian Banks

The fifth EBG principle for e-banking risk management states that banks should use transaction authentication methods that promote non-repudiation[5] and establish accountability for e-banking transactions. 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 has been received or to protect the recipient against false denial by the sender that the data has 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 or e-banking users to claim that transactions were fraudulently altered (Basel Committee 2003).

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.

[5] 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

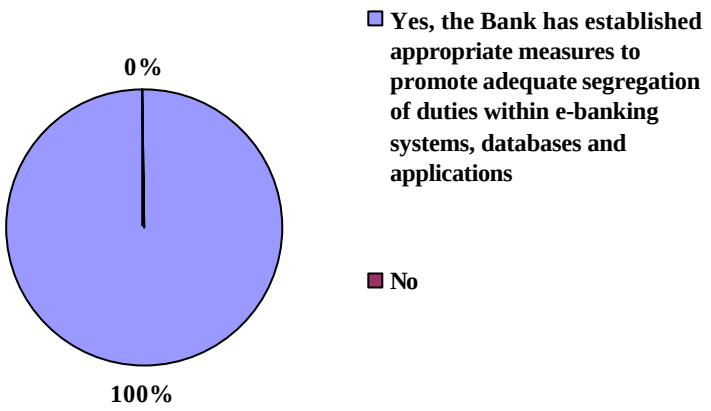

Figure 12. The Application of Appropriate Measures to Ensure Segregation of Duties at the Estonian Banks

Segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems and 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. 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 (Basel Committee 2003).

According to the results of the questionnaire, all Estonian banks have established appropriate measures to promote adequate segregation of duties within e-banking systems, databases and applications.

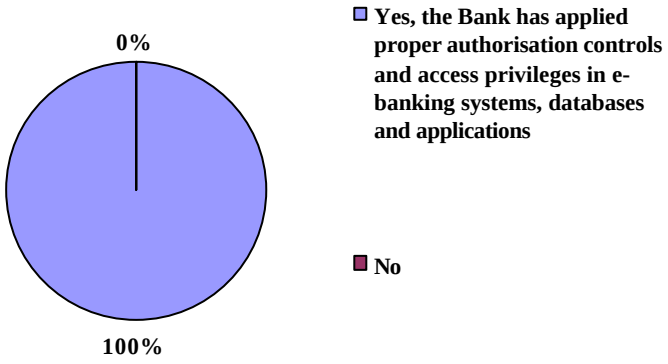

Figure 13. The Existence of Proper Authorisation Controls at the Estonian Banks

In order to maintain segregation of duties, banks need to strictly control authorisation and access privileges. 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 (Basel Committee 2003).

According to the Estonian e-banking specialists, all banks have applied proper authorisation controls and access privileges in e-banking systems, databases and applications.

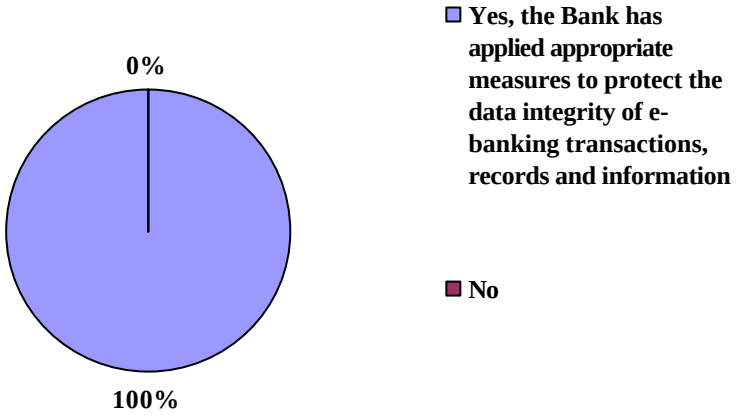

Figure 14. Protection of the Data Integrity in E-Banking at the Estonian Banks

Failure to maintain the data integrity[6] 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, all banks have applied appropriate measures to protect the data integrity of e-banking transactions, records and information.

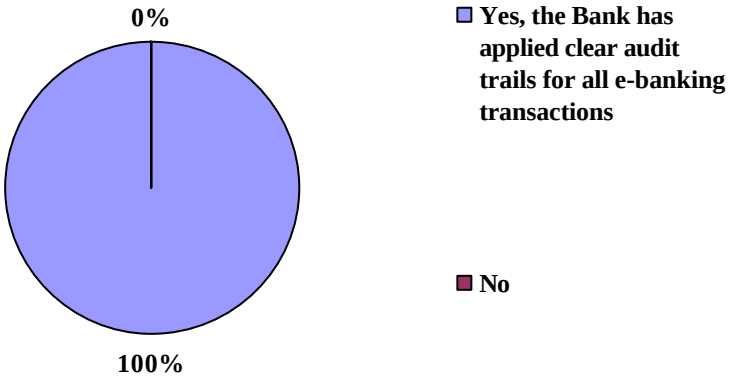

Figure 15. Application of Audit Trails for E-Banking Transactions at the Estonian Banks

[6] Data integrity is the state of data in case destructions, undesirable changes and losses are missing

Delivery of financial services over the Internet can make it more difficult for banks to apply and enforce internal controls and maintain clear audit trails[7] 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. This is because much, if not all, of its records and evidence supporting e-banking transactions are in an electronic format (Basel Committee 2003).

In their responses to the e-banking risk management questionnaire all banks have stated that clear audit trails have been implemented for all e-banking transactions.

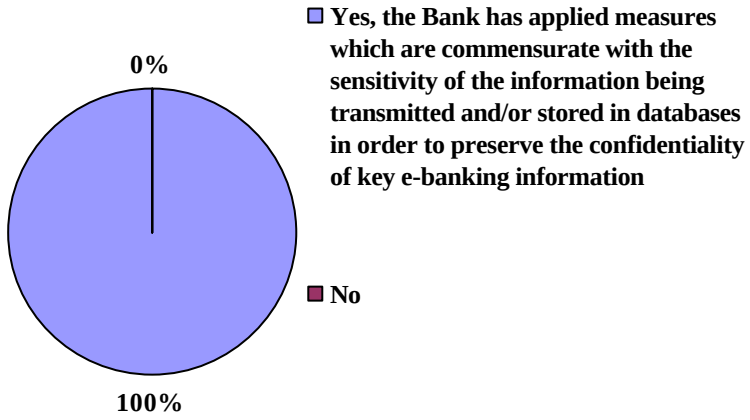

Figure 16. Confidentiality of Key E-Banking Information at the Estonian Banks

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. Additionally, increased use of service providers may expose key bank data to other parties (Basel Committee 2003).

In Estonia, according to the banks' responses, 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.

7. Legal and Reputational Risk Management in Estonia

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers

[7] 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

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 .

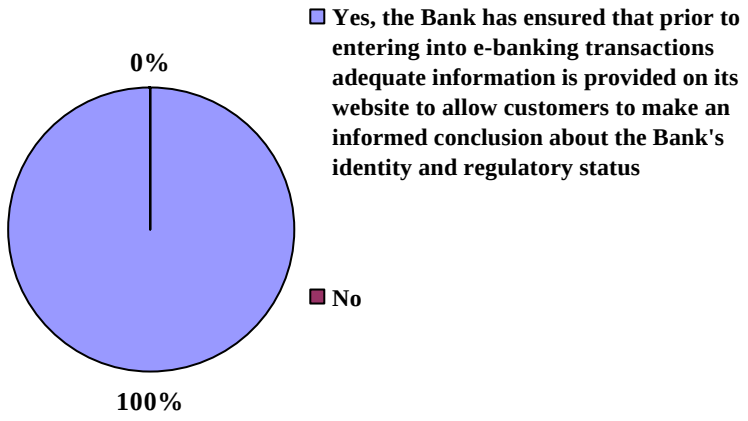

Figure 17. Provision of Adequate Information to Customers Prior to E-Banking by the Estonian Banks

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 to 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 to make an informed conclusion about the bank identity (e.g. contact details, customer support, information on the offered e-products' and e-services' conditions) and regulatory status.

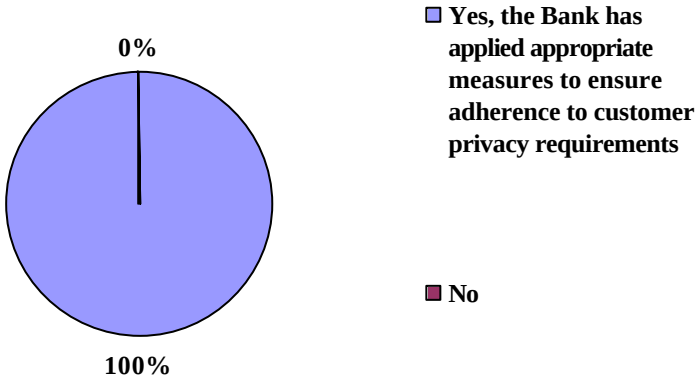

Figure 18. Compliance with Customer E-Banking Privacy Requirements at the Estonian Banks

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, all banks in Estonia have applied appropriate measures to ensure adherence to customer privacy requirements.

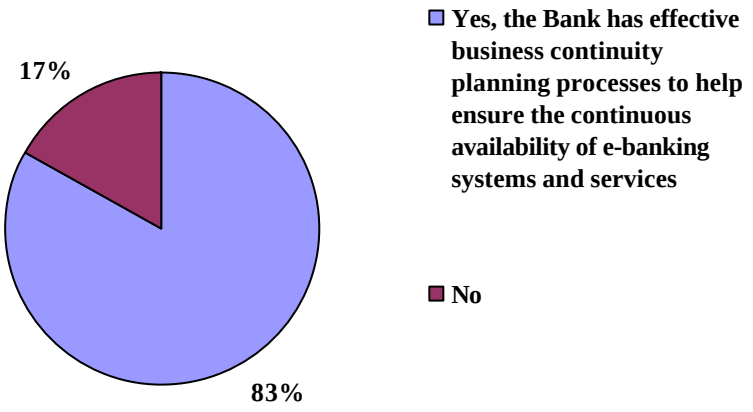

Figure 19. The Existence of Capacity, Business Continuity and Contingency Planning at the Estonian Banks

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 banks have established effective capacity, business continuity and contingency planning processes to help ensure the continuous availability of e-banking systems and services. Only 2 banks do not have operational business continuity planning processes whereby one bank is currently making active preparations to establish them.

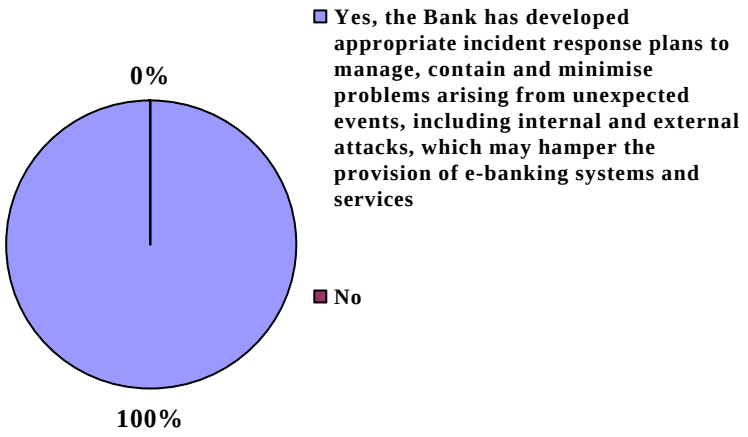

Figure 20. Incident Response Planning at the Estonian Banks

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.

8. Conclusions

In order to assess the regional development of e-banking in Estonia, the author conducted a special survey in the form of questionnaire which made it possible to assess the distribution of payment instruments by five regions.

According to the Eesti Pank (Bank of Estonia) Governor's Decree No. 9 of 9 October 2003, the Bank of Estonia collects payment statistics from the credit institutions licensed in Estonia and branches of foreign credit institutions (hereinafter *banks*). However, for the needs of the survey it was not possible to use the reports collected by the Bank of Estonia for two reasons. First, these reports do not have a regional component, e.g. they contain the data on the whole Estonia, but not on its regional units. Second, the classification of payment instruments in these reports is somewhat different – e.g. it is not possible to identify the payments via bank branches.

Currently there are fourteen banks operating in Estonia of which eleven are obliged to submit payment reports to the Bank of Estonia. Consequently, the author contacted only these eleven banks' accountants or reporting specialists and asked them to provide the data on the number of payment instruments by three consecutive years: 2004, 2005 and 2006. The payment instruments for the needs of the future analysis in this research were classified differently from the Bank of Estonia's

classification. The banks were asked to fill in six tables: distribution of payment instruments during the period of 2004-2006 in the total Estonia, Northern Estonia, Western Estonia, Central Estonia, North-Eastern Estonia and Southern Estonia.

Six banks out of eleven sent the filled-in questionnaires back, thus making the response rate of 55%. Taking into account the high concentration of the Estonian banking market and the certain limitations of the data collection, the author considers the response rate to be good. Also, among the banks which have responded to the questionnaire were several banks with banking activities throughout the whole Estonia. That is why it was possible to extend the results of the survey to the whole Estonian banking sector.

Having aggregated banks' responses, the author has analysed the usage of different payment instruments in Estonia as a whole as well as in its five regions. To conclude, it could be stated that the usage of e-banking channels which consist of card payments via ATM or at POS, direct debit, standing order, telebank, telephone bank, Internet bank and mobile phone payments is quite uniform in all five regions constituting 94%-97% of all payments. The share of payments via bank branches during the last three years (2004-2006) has declined in all five regions. The largest share of bank branches is in the North-Eastern Estonia, 5.8%.

If we make international comparisons and compare the regional distribution of payment instruments in Estonia with that in Finland, we can notice that in general the usage of e-banking in Estonia is very high like in Finland. However, in Finland, the share of e-banking channels is the highest at the capital region (around 93%) and the lowest in the countryside (around 83%), e.g. the significance of branch offices is quite large there compared to the capital region. In this respect, the regional distribution of payment instruments is more even in Estonia where in all regions the share of e-banking channels varies insignificantly.

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 the 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 the 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.

According to the previous research, the major concern for e-banking customers is the security of e-channels. Consequently, 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

Basel Committee on Banking Supervision (2003). Risk Management Principles for Electronic Banking.

BIS (2004). Survey of Developments in Electronic Money and Internet and Mobile Payments.

Changgyu, A. (2003). Eestil head eeldused haarata juhtpositsioon. In: Äripäev Online, 17.06.2003.

Crockett, A. (2001). Financial Stability in the Light of the Increasing Importance of Online-Banking and E-Commerce. BIS Review 5/2001.

Danish Management (2004). Central and Eastern Europe Information Society Benchmarks. Country Analysis.

Eesti Pank (2003). Eesti Pank Governor's Decree No. 9. Confirmation of Reports on Payments Statistics Submitted by Credit Institutions.

Estonian Banking Association (2003). Estonian Commercial Banks: Brief History 1988-2001.

Finnish Bankers' Association (2004). Banking Technology in Finland..

Glaessner, T. (2003). Electronic Safety and Soundness: Securing Finance in a New Age. Public Policy Issues. The World Bank.

Nsouli, S. (2002). Challenges of the "E-Banking Revolution". In: IMF Finance & Development, vol. 39, no. 3.

Schaechter, A. (2002). Issues in Electronic Banking: An Overview. IMF Policy Discussion Paper PDP/02/6.

Schilder, A. (2001). Banking in the New Economy: A Supervisory Perspective. BIS Review 16/2001.

Sergeant, C. (2000). E-Banking: Risks and Responses. Financial Services Authority.

Ülevaade WWW-lehekülgedest (2000). Available at: http://www.esis.ee/Q5/EewwwQ5_inEST.html