Study of factors affecting operational electronic banking risks in Iran (Case Study: Melli bank of Kermanshah)

Peyman Akbari¹, Rezvan Rezavandi², Toraj Vatandost³, Omid Baharestan⁴

1. Master of Commercial Management, Young Researchers Club, Kermanshah Branch, Islamic Azad University Kermanshah, Iran
2. Master of Commercial Management financial trend, Islamic Azad University, Kermanshah Branch, Iran
3. Master of Commercial Management financial trend, Islamic Azad University, Kermanshah Branch, Iran
4. Master of Commercial Management, Esfahan University, Esfahan, Iran

Corresponding author email: peymanakbari3537@yahoo.com

ABSTRACT: Recently, banks have been providing their electronic services to customers remotely. This technological innovation by E-banking systems has been accompanied by several risks in addition to benefits it has brought about to customers one of which is operational risks. Banks need to identify this risk in order to manage it. Present research identifies, compares, and ranks factors affecting operational E-banking risks in viewpoints of customers and employees of Kermanshah Melli bank. To this end, a questionnaire was distributed to 300 employees and 384 customers of Kermanshah Melli bank randomly cluster. The method of this study is descriptive- survey research. The first half of the year of 2012 constituted study period. One-Sample T-Test, Friedman ranking Test and Independent Samples Test were employed to test hypotheses, to rank factors affecting operational risks and Comparison the amount of effective factors on the operational risks of electronic banking at Melli Bank of among employees and customers, respectively results indicate that hypotheses (1-5) support effects the factors (data accuracy, internal controls, technological infrastructure, access to systems, and security) have on Melli bank operational E-banking risks; hypothesis (6) Ranks each of the 5-fold factors are not equal and In factors (Security), employees opinion is more than customers,. But In factors (Data accuracy, Technological infrastructures, Access to systems), customers opinion is more than employees. This research concludes with some recommendations to Kermanshah Melli bank in order to manage and lower operational E-banking risks.

Keywords: data accuracy, internal controls, technological infrastructure, access to systems, security, operational risks, E-banking.

INTRODUCTION

Application of E-banking seems to be an essential task given the recent world transformations and societies turning to E-business and using internet and electronic facilities instead of using traditional methods. Nowadays, banking industry is changing quickly banks have been influenced by international economy development and market competition; and development of information and communication technology and increasing growth of electronic transaction and business across the world and business need for presence of banks to transfer financial resources all have made E-banking on integral part of E-business, which plays a crucial role in its implementation. It can be said boldly that E-business is not realized without E-banking. Recent business transformations have raised new concepts in E-banking, including fund electronic transfer, bank cards, electronic money electronic payment of bills automated clearinghouse, etc.(Money & bank research center, 2005). In addition, innovations such as telecommunication networks, cell phones, internet automated teller machines (ATM), automatic branches, electronic money, and so on have changed ways of service providing by banks and financial institutions, on one hand and have provided banks with such advantages as focusing on new distribution channels, having access to services provided by banks with no spatial – time constraints.
limitations, more geographically covered areas, possibility of \textsuperscript{3}E-shopping, and possibility of having access to
and monitor personal accounts, on the other, which have increased banks competition power within today’s
complex markets. New risks caused by this phenomenon are employees and customers unfamiliarity with new
technology, lack of infrastructures necessary to provide \textsuperscript{4}E-services. Not taking an appropriate strategic
approach by bank managers and by governmental top managers; these are challenges facing banks and
financial institutions. One of the most important responsibilities of management of banks and financial
institutions is to understand all kinds of risk and to take a management strategy to reduce them. So it can be
claimed that movement from manual to entirely computer processing accompanied by increased processing
volume, whether in number or is source, is the most concerning problem of current era because it has raised
risk likelihood and reduced control over such transactions (Sheykhani, 1999). Therefore, it is necessary for
financial institutions to be flexible in order to face future world’s challenges and changes successfully.
Professional risk management is one of the most important domains requiring adaptation of financial institutions
to new conditions in order for it to understand increasing complexity caused by regulations, customers, and
technology and to act efficiently. Without such adaptation, undoubtedly, an institution is most likely to encounter
conditions threatening its continuous activity and survival (El-Kharouf and Magdalena, 1999). These factors led
a committee called Basel to begin preliminary studies on risk management principles in E-banking and \textsuperscript{5}E-
money areas in 1998, which specified necessity of more work in risk management domain the result of which
was establishment of a working group, named E-banking group, consisting of the heads of banks and central
banks in Nov. of 1999. Report of this group on risk management and topics if E-banking supervision was
approved by basal committee in Oct of 2000. According to this report, main E-banking risks include strategic,
credit, operational, liquidity, and market risks (Basel Committee, 2003). Given that people have already turned
to, or are now turning to, the use of E-banking services, to identify risks associated with this type of banking is
considered an essentially important task so that banks and financial institutions be able to encourage people to
use such banking more and more by identifying and reducing related risks. As mentioned earlier, operational
risks are one of major risks known in E-banking services which is not a new phenomenon, but its importance
has been highlighted recently with spread of information technology application (so that Basel committee has
issued numerous instructions and reports to facilitate operational risk management, although technology has
facilitated performing of many organizational tasks and more importantly, resulted in productivity growth, it has
brought about new problems for organizations the most important of which is operational risks). So banks need
to be highly attendant in this regard since in the case operational risks are not managed well, they will lead to
not only economic losses but also banks bankruptcy (Money & bank research center, 1999). To this end, the
first step is to identify factors creating such risks in order to reduce intensity of such risks and to manage them
better by controlling and lowering the level of these factors influence. Now given problems like ATM;
telecommunication lines, and technological infrastructures inefficiency, this phenomenon has created in our
country, it should be seen that, as a financial institution providing bank services, what factors must Kermanshah
Melli bank consider to manage such risks in order to lower its operational risks? And what steps must it take to
prevent risks and abuses? Ultimately, this research seeks to compare the levels of influence said factors have
on operational E-banking risks in viewpoints of employees and customers of Kermanshah Melli bank.

\textbf{According to the above, Research carried out related to electronic banking and operational risks of
electronic banking as follows}

Sokolov (2008) examined operational E-banking risks in Estonian banks. Results indicated that security
controls, periodic check of individuals with key positions, and limited unauthorized access to E-banking data are
the most important factors affecting operational \textsuperscript{5}E-banking risks.

\textbf{Chang and Twang (2007)}

investigated factors influencing internet security in Taiwanese banks. They found that security is one of
the most important reasons for adoption and application of internet banking.

\textbf{Shakeri (2007)}

studied vital factors of success of Iranian E-banking in the form of external (managerial, socio-cultural,
technological, economic ones) and internal (telephone banking, internet banking ATM, and sale-point
machines) factors. Results indicated that technological and socio-cultural factors are the most important
external factors, and management of ATM bank operations POS security systems, organizational structures of
telephone and internet banking are the most important internal ones.

\textsuperscript{3} Electronic Shopping
\textsuperscript{4} Electronic Services
\textsuperscript{5} Electronic Money
Kesheh farahani (2007) studied and evaluated approaches to transition from traditional to E-banking in Persian bank. Results showed that basic infrastructures are the most important obstacles to Iranian E-banking followed by legal, social, and cultural factors, obstacles related to technological knowledge, economic factors, and internal bank factors.

Hamidizadeh et al. (2006) identified and ranked challenges and hardships of environments external to Iranian E-banking system. They found that low speed of communicational networks, internet infrastructures, low level of customers knowledge and awareness management problems, sites maintenance, incompatibility of traditional banking with electronic one, and insecure communication systems and networks are among main challenges to development of E-banking.

Karimi (2006) identified and studied factors affecting the risks of sepah bank information security. This researcher identified 4 elements as factors affecting the risks of sepah bank information security: (1) data classification (confidentiality authenticity, access ability), (2) management controls (risk management, revision of security controls, life cycle running, business continuation planning, and error correction), (3) operational controls (personnel security, environmental / physical security, documentation, awareness of and training security), and (4) technical controls (identification and certification of identity and non-denial, logical access control, audit of registration and monitoring).

Ayady (2006) divided factors influencing establishment of E-banking in Tunisia into 2 technological and organizational ones. He considers such factors as central architecture, multiple information systems, organizational inflexibility, and ignoring users wants as being effective in failed E-banking establishment.

Aghaunor and Fothoh (2006) examined factors effective in applying E-business to Nigerian commercial banks. Results showed that top management support; organizational capabilities; technological infrastructures; perceived interests, compatibility, and complexity; supporting industries; and government support are factors effective in establishment of E-banking within Nigerian commercial banks.

Watangase (2005) addressed management roles within Thailand banks it environment. He identified security, data confidentiality, data accuracy. System integration, internal controls, and Outsourcing as factors influencing operational E-banking risks.

Venus and Salehi (2004) identified factors influencing customer's tendency to use bank automatic payment systems. Results showed that spatial desirability, customer awareness, system integration, service diversity, easy use, availability and reliability are 6 factors influencing customer tendency to use bank automatic payment systems.

Pilawski (2003) examined obstacles to establishment and implementation of E-banking within polish banks. He introduced security data confidentiality, technological infrastructures, data accuracy, internal controls, and Outsourcing as factors influencing operational E-banking risks.

**Research hypotheses**

Hypotheses1: Data accuracy influences operational E-banking risks in Melli bank of Kermanshah.

Hypotheses2: Internal controls influence operational E-banking risks in Melli bank of Kermanshah.

Hypotheses3: Technological infrastructures influence operational E-banking risks in Melli bank of Kermanshah.

Hypotheses4: Access to systems influence operational E-banking risks in Melli bank of Kermanshah.


Hypotheses6: Are there significant differences among use rate of each of the five factors?
MATERIALS AND METHODS

The present study is descriptive-surveys research which is one of applied research. Required information of research literature sector has been gathered from books, specialized journals articles on Persian (ISC) and Latin derived (library methods). For data collection has been used the questionnaire designed with Likerts spectrum was researchers made which includes 24 questions. Validity of the questionnaire was confirmed by a group of university professors. And for determined reliability of the questionnaire was used Cronbach's alpha 0.747 for employees and 0.813 for customers. Finally, the collect information to calculate variables research was stored in a database such as Excel (field method). One-Sample T-test was used to analyze data for testing research hypotheses. And Friedman's ranking test was used to rank factors influencing operational risks in viewpoints of employees and customers and Independent T-test to compare the degree of each of 5 factors influence in points of view of employees and customers. In the 95% confidence level, and P-value<5%, Hypothesis is confirmed (H_1) and otherwise (H_1) is rejected. In addition to set the statistical tables, statistical data analysis, was used Spss software. The statistical population is 300 employees and 384 Customers of Melli Bank of Kermanshah; for a period of 6 months of first half of 2012, were selected randomly clusterly.

Hypothesis1
Data accuracy influences operational E-banking risks in Melli bank of Kermanshah. Given that sig level is smaller than 5% error one it can be said that H_1 is accepted. Therefore, with 95% confidence, factor of data accuracy has influence on operational E-banking risks in Melli bank of Kermanshah in viewpoints of employees and customers. Also, results show that, with 95% confidence interval, mean of the effect of importance of data accuracy on operational E-banking risks among employees and customers of Kermanshah Melli bank Lies between (10.1346 and 10.9121) and (13.6548 and 14.3244).

Hypothesis2
Internal controls influences operational E-banking risks in Melli bank of Kermanshah. Given that sig level is smaller than 5% error one it can be said that H_1 is accepted. Therefore, with 95% confidence, factor of internal controls has influence on operational E-banking risks in Melli bank of Kermanshah in viewpoints of employees and customers. Also, results show that, with 95% confidence interval, mean of the effect of importance of internal controls on operational E-banking risks among employees and customers of Kermanshah Melli bank Lies between (14.6615 and 15.3718) and (14.4934 and 15.2722).

Hypothesis3
Technological infrastructures influences operational E-banking risks in Melli bank of Kermanshah. Given that sig level is smaller than 5% error one it can be said that H_1 is accepted. Therefore, with 95% confidence, factor of Technological infrastructures has influence on operational E-banking risks in Melli bank of Kermanshah in viewpoints of employees and customers. Also, results show that, with 95% confidence interval, mean of the effect of importance of Technological infrastructures on operational E-banking risks among employees and customers of Kermanshah Melli bank Lies between (16.4222 and 17.3312) and (21.2400 and 22.2183).

Figure 1: Research conceptual model
**RESULTS OF TESTING HYPOTHEZE**

**Table 1. T-Test**

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Std. Error Mean</th>
<th>t</th>
<th>df</th>
<th>Sig. (2-tailed)</th>
<th>Mean Difference</th>
<th>95% Confidence Interval of the Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lower</td>
</tr>
<tr>
<td>1</td>
<td>300</td>
<td>13.5233</td>
<td>3.42177</td>
<td>0.19756</td>
<td>53.268</td>
<td>299</td>
<td>0.000</td>
<td>10.52333</td>
<td>10.1346</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>16.9896</td>
<td>3.33662</td>
<td>0.17027</td>
<td>82.161</td>
<td>383</td>
<td>0.000</td>
<td>13.98958</td>
<td>13.6548</td>
</tr>
<tr>
<td>2</td>
<td>300</td>
<td>18.0167</td>
<td>3.12553</td>
<td>0.18045</td>
<td>83.217</td>
<td>299</td>
<td>0.000</td>
<td>15.01667</td>
<td>14.6615</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>17.8828</td>
<td>3.88064</td>
<td>0.19803</td>
<td>75.153</td>
<td>383</td>
<td>0.000</td>
<td>14.88281</td>
<td>14.4934</td>
</tr>
<tr>
<td>3</td>
<td>300</td>
<td>19.8767</td>
<td>4.00018</td>
<td>0.23095</td>
<td>73.075</td>
<td>299</td>
<td>0.000</td>
<td>16.87667</td>
<td>16.4222</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>24.7292</td>
<td>4.87543</td>
<td>0.24880</td>
<td>87.337</td>
<td>383</td>
<td>0.000</td>
<td>21.72917</td>
<td>21.2400</td>
</tr>
<tr>
<td>4</td>
<td>300</td>
<td>13.8533</td>
<td>3.43674</td>
<td>0.19842</td>
<td>54.699</td>
<td>299</td>
<td>0.000</td>
<td>10.85333</td>
<td>10.4629</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>16.6615</td>
<td>3.88946</td>
<td>0.19848</td>
<td>68.829</td>
<td>383</td>
<td>0.000</td>
<td>13.66146</td>
<td>13.2712</td>
</tr>
<tr>
<td>5</td>
<td>300</td>
<td>27.6100</td>
<td>3.19561</td>
<td>0.18450</td>
<td>133.388</td>
<td>299</td>
<td>0.000</td>
<td>24.61000</td>
<td>24.2469</td>
</tr>
<tr>
<td></td>
<td>384</td>
<td>25.2760</td>
<td>4.76024</td>
<td>0.24292</td>
<td>91.701</td>
<td>383</td>
<td>0.000</td>
<td>22.27604</td>
<td>21.7984</td>
</tr>
</tbody>
</table>

**Table 2. Friedman -Test**

<table>
<thead>
<tr>
<th>Sig</th>
<th>df</th>
<th>Chi-Square</th>
<th>Mean Rank</th>
<th>N</th>
<th>NO</th>
<th>Variable</th>
<th>hypothesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000</td>
<td>4</td>
<td>964.648</td>
<td>4.96</td>
<td>300</td>
<td>5</td>
<td>Security</td>
<td>employees</td>
</tr>
<tr>
<td>0.000</td>
<td>4</td>
<td>1059.954</td>
<td>1.96</td>
<td>384</td>
<td>5</td>
<td>Access to systems</td>
<td>Customers</td>
</tr>
<tr>
<td>1.61</td>
<td>300</td>
<td>1</td>
<td>Data accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.74</td>
<td>300</td>
<td>2</td>
<td>Access to systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.11</td>
<td>300</td>
<td>3</td>
<td>Internal controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.58</td>
<td>300</td>
<td>4</td>
<td>Technological infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.88</td>
<td>384</td>
<td>1</td>
<td>Access to systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.93</td>
<td>384</td>
<td>2</td>
<td>Data accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.42</td>
<td>384</td>
<td>3</td>
<td>Internal controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.36</td>
<td>384</td>
<td>4</td>
<td>Technological infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.39</td>
<td>384</td>
<td>5</td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 3. T-Test

<table>
<thead>
<tr>
<th>Group</th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Std. Error Mean</th>
<th>Levene's Test for Equality of Variances</th>
<th>T-Test for Equality of Means</th>
<th>95% Confidence Interval of the Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lower</td>
</tr>
<tr>
<td>1</td>
<td>Employees</td>
<td>300</td>
<td>13.5233</td>
<td>3.42177</td>
<td>0.19756</td>
<td>Equal variances assumed</td>
<td>5.755</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>384</td>
<td>16.9896</td>
<td>3.33662</td>
<td>0.17027</td>
<td>Equal variances not assumed</td>
<td>-13.290</td>
</tr>
<tr>
<td>2</td>
<td>Employees</td>
<td>300</td>
<td>18.0167</td>
<td>3.12553</td>
<td>0.18045</td>
<td>Equal variances assumed</td>
<td>12.208</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>384</td>
<td>17.8828</td>
<td>3.88064</td>
<td>0.19803</td>
<td>Equal variances not assumed</td>
<td>0.500</td>
</tr>
<tr>
<td>3</td>
<td>Employees</td>
<td>300</td>
<td>19.8767</td>
<td>4.00018</td>
<td>0.23095</td>
<td>Equal variances assumed</td>
<td>2.196</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>384</td>
<td>24.7292</td>
<td>4.87543</td>
<td>0.24880</td>
<td>Equal variances not assumed</td>
<td>-14.294</td>
</tr>
<tr>
<td>4</td>
<td>Employees</td>
<td>300</td>
<td>13.8533</td>
<td>3.43674</td>
<td>0.19842</td>
<td>Equal variances assumed</td>
<td>6.476</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>384</td>
<td>16.6615</td>
<td>3.88946</td>
<td>0.19848</td>
<td>Equal variances not assumed</td>
<td>-10.006</td>
</tr>
<tr>
<td>5</td>
<td>Employees</td>
<td>300</td>
<td>31.3951</td>
<td>3.19561</td>
<td>0.18450</td>
<td>Equal variances assumed</td>
<td>15.092</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>384</td>
<td>25.2760</td>
<td>4.76024</td>
<td>0.24292</td>
<td>Equal variances not assumed</td>
<td>7.651</td>
</tr>
</tbody>
</table>
**Hypothesis 4**

Access to systems influences operational E-banking risks in Melli bank of Kermanshah. Given that sig level is smaller than 5% error one it can be said that $H_1$ is accepted. Therefore, with 95% confidence, factor of Access to systems has Influence on operational E-banking risks in Melli bank of Kermanshah in viewpoints of employees and customers. Also, results show that, with 95% confidence interval, mean of the effect of importance of Access to systems on operational E-banking risks among employees and customers of Kermanshah Melli bank Lies between (10.4629 and 11.2438) and (13.2712 and 14.0517).

**Hypothesis 5**

Security influences operational E-banking risks in Melli bank of Kermanshah. Given that sig level is smaller than 5% error one it can be said that $H_1$ is accepted. Therefore, with 95% confidence, factor of Security has Influence on operational E-banking risks in Melli bank of Kermanshah in viewpoints of employees and customers. Also, results show that, with 95% confidence interval, mean of the effect of importance of Security on operational E-banking risks among employees and customers of Kermanshah Melli bank Lies between (24.2469 and 24.9731) and (21.7984 and 22.7537).

(Question) **Hypothesis 6**

Are there significant differences among of each of the five factors on operational electronic banking risks?

Ranks each of the 5-fold factors are equal. $H_0$: $P_1 = P_2 = ... = P_5$

There is a significant difference between at least 2 of ranks of factors affecting operational electronic banking risks? $H_1$: $P_1 \neq P_2 \neq ... \neq P_5$

Given means and ranking means of each calculated factor, variable which has the least influence gains the lowest ranking. According to table 2, for both employees and customers freedom degree is 4 and significance level is. 000, but $x^2$ is 964.648 for the employees and 1059.954 for the customers. Since significance level is < 5% both employees and customers $H_1$ is accepted, therefore, there is a significant difference among means of factors. Thus, factors influencing operational E-banking risks in Melli bank are, in viewpoints of employees and customers, in low-to-high influence order as follows:

**In viewpoints of employees**

- Data accuracy, access to systems, internal controls, technological infrastructures, and security.

**In viewpoints of customers**

- Access to systems, data accuracy, internal controls, technological infrastructures, and security.

**Note Table 3: T-Test**

Comparison the amount of effective factors on the operational risks of electronic banking at Melli Bank of Kermanshah among employees and customers

- H0: mean of factors affecting operational electronic banking risks between staff and customers is equal.
- H1: mean of factors affecting operational electronic banking risks between staff and customers is not equal.

Given that sig levels is smaller than 5% error one it can be said that $H_1$ is accepted. Only In Internal controls factor is reject because the test significance level (equal to 0.627) is More than 5%. In the end: in factors (Security), mean of employees group is higher than customers group. So we conclude that the amount of factors affecting on operational risks of electronic banking according to employees opinion is significantly more than customers.

In factors (Data accuracy, Technological infrastructures, Access to systems), mean of customers group is higher than employees group. So we conclude that the amount of factors affecting on operational risks of electronic banking according to customers opinion is significantly more than employees.

**RESULTS AND DISCUSSION**

On the basis of hypotheses (1-5) and of research tests, it is concluded that all 5 factors influence operational E-banking risks in Kermanshah Melli bank.

Based on hypothesis (6) and on research tests, it is concluded that factor of security is of the highest effect on operational E-banking risks in Melli bank of Kermanshah followed by access to systems, technological infrastructures, internal controls, and data accuracy. Given the importance employees and customers of Melli bank place on these factors, thus, it is expected that this bank to have more careful and stronger strategies and approaches to these factors.
Findings

of this research show that these 5 factors influence operational E-banking risks in Melli bank of Kermanshah. Results of this research are in line with previous ones findings.


Sokolov (2008), Pilawski (2003), and Venus & salehi (2004) identified access to systems as a factor influencing operational E-banking risks.


Karimi (2006), Watanagase (2005), and Pilawski (2003) identified factors of data accuracy and internal controls as those influencing E-banking.

Recommendations

Research recommendations are presented in 2 parts. First, includes applied suggestions related to management of operational risks in Melli bank E-banking system and second, includes suggestions for future research.

1. Given the results of present research, it is suggested that Melli bank management embark on creating a database to get precise information on studied factors in order to manage operational risks better within its own E-banking system for defining its E-banking processes, transactions, and functional areas in short term. It is evident that at the end of this period bank management will be able to formulate efficient policies and strategies for risk management considering available data and specified priorities.

2. For data accuracy, it is recommended that Melli bank plan & program office document all its E-banking processes and examine them technically managerially while revising and redefining them optimally in order to organize Melli bank E-banking processes logically properly. By doing so, bank needs related to the process of data management are identified based on which software correcting incorrect data is designed and developed.

3. For internal controls, it is suggested that this bank define sufficient logs for all steps if E-banking transaction process, intercepting and controlling whole transactions. Also, it is recommended that multiple methods be used simultaneously to identify users while being connected to servers and databases. To control employees, it is suggested that whole bank personnel be classified based on their organizational positions and information requirements commensurate with those positions; and informational level of and access level to Melli bank E-banking systems be defined commensurate with each class and users be allowed to to have access only to specified levels, for servers, systems, and databases, it is suggested that an efficient contingency program be defined, duties of each employee be determined clearly while training them in order to prevent any disruption in providing services caused by natural disasters (flood, earthquake, storm, etc.) and intentionally mistakenly human – made unpredicted incidents. One important point in this field is to prepare supporting systems and data banks being updated and to place them in locations geographically different from those of main servers and databases.

4. For technological infrastructures, it is recommended that the bank choose technologies and systems in such a manner that they not only comply with common standards of banking industry but also be capable of achieving bank strategic outlooks in direction of providing services to customers effectively flexibly. An effective solution to reduce risks related to this area is to hold negotiations among central bank, banks representatives, and organizations concerned (communications & technology, telecommunications, power, etc.) in order to examine weaknesses of these organizations and to appoint groups to improve status quo. It is suggested that Melli bank use Linux operating system, developed form of UNIX operating system, so that it can be made indigenous easily. It should be noted that many countries which are not willing to establish commercial relationships with the U.S. and/or are under sanction turn to this operating system. This operating system is advantageous because it is no organizations monopoly, that is, it has not been produced by a particular manufacturer, but evolved by different specialists. Also it should be pointed out that according to experts, inappropriate infrastructures of telecommunication and a communicational network is among factors problematic in the field of E-banking. Positive steps can be taken to reduce E-banking risks by improving these infrastructures and by increasing seed and precision of communicational networks.
5. For access to systems, it is suggested that tasks related to E-banking processes be divided carefully with a preventive logic; all changes in access limits be registered and recorded, requiring approval by bank top management, and controlling, monitoring, and inspecting units. Also, employees activities need to be controlled both regularly tangibly and accidentally intangibly job rotation and employee exchange is another control policy being effective in reducing operational losses caused by employees. This problem can be resolved by providing employees with continuous education and by occupational planning although financial institutions are reluctant to hold posts related to E-banking activities due to necessity of high specialty. Also, it is suggested that similar policies be applied to bank external users (customers) in order that merely authorized users be able to do allowed operations and transactions within specified and defined limits. Among procedures proposed to control users access to banks E-baking systems is to change passwords periodically and to control and intercept transactions of E-banking irregularly accidentally.

6. For security, it is suggested that Melli bank design and implement a careful and strong security policy for bank employees, which is active in units related to E-banking. Also, it is recommended that this bank management outsource required software system by concluding valid and appropriate contracts with valid foreign companies given the lack of antivirus software and software protecting against unauthorized penetration to network inside country, of course, it needs to gain necessary implementation guarantee for updating and supporting related tasks by those companies.

finally, given opinions and suggestions expressed by it assistants and employees working for this sector in Kermanshah during interviews performed, it needs to be pointed out that banks and financial institutions need to offer more comprehensive education to customers using E-banking services in order to minimize risks in such banking by training and creating a proper culture among general public.

The second part gives some recommendations to interested researchers for future research:
1- To examine other factors like outsourcing as one influencing operational E-banking risks. Thus, interested individuals could examine each of factors studied in present research separately for Melli and/or any other national banks by defining standards more precise than and beyond minimal specified here.
2- To study approaches to calculation of capital sufficiency comparatively for operational risks in Melli bank E-banking systems.
3- To identify, study, and provide the most efficient standards of monitoring and supervision based on the second element of instructions of Basel committee for Iranian E-banking system.
4- To examine factors influencing credit and market risks in Melli bank and to design measurement model for liquidity risks for Melli bank banking system and, finally; to suggest an efficient and effective risk management regime for Melli bank.

REFERENCES
Aghaunor L, Fothoh X. 2006. Factors effecting Ecommerce adoption in Nigerian Banks. JIBC.
Kesheh farahani S. 2007. Study and evaluation of approaches to transition from traditional to electronic banking in Iran and to provide a suitable case study approach of Persian bank. M.A. dissertation of Tehran university of Iran.
Money & bank research center 2005. Electronic banking and its administrative requirements in comparison of operational costs of different banking services. spring. Center Bank of Iran (text Persian)
Money & bank research center, 1999. E-banking and its strategies in Iran" winter. Center Bank of Iran (text Persian)
Sheykhani S. 1999. Electronic banking and its strategies in Iran. money and bank research agency Tehran. (text Persian)