“An investigation of risk management practices in electronic banking: the case of the UK banks”

AUTHORS	Hussein A. Abdou https://orcid.org/0000-0001-5580-1276 John English Paul O. Adewunmi

ARTICLE INFO	Hussein A. Abdou, John English and Paul O. Adewunmi (2014). An investigation of risk management practices in electronic banking: the case of the UK banks. *Banks and Bank Systems*, *9*(3)
JOURNAL	"Banks and Bank Systems"
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES **0**

NUMBER OF FIGURES **0**

NUMBER OF TABLES **0**

Hussein A. Abdou (UK), John English (UK), Paul O. Adewunmi (UK)

An investigation of risk management practices in electronic banking: the case of the UK banks

Abstract

This paper investigates the risk management practices in e-banking of major UK banks, using the framework of principles introduced by the Basel Committee on Banking Supervision (BCBS). The initial pilot study involves four interviews conducted with staff members of one of the leading UK banks on risk management for e-banking. The main research instrument is a questionnaire divided into three sections covering board management and oversight, security controls and legal and reputational risk management. The questionnaire is used across ten major UK banks to establish whether they are operating in line with these risk management principles. The interviewees suggest that the main risk to customers using e-banking is security risk and that the bank is focusing on mitigating that risk. Our findings from the questionnaire indicate that the UK banks have successful risk management systems that help to stop potential electronic risk and reduce the losses incurred from risks associated with e-banking. Our results also confirm that UK banks are complying with the 14 BCBS risk principles and are well managed in terms of their security controls for e-banking. With the continued phenomenal growth and investment into e-banking the authors recommend that UK banks must avoid a repetition of the recent complacencies seen with on-line payments, corporate governance issues and the rising tide of complaints, that are referred to the financial ombudsman. They must also ensure they keep up-to-date security systems to reduce the security risk to different parties and that staff members are fully trained on legal and reputational risk management practices.

Keywords: e-banking, risk management, security risk, UK.
JEL Classification: C22, E44, G21.

Introduction

The growth in use of the Internet has seen radical changes in the way banks operate with the number of customers using cyber banking growing to 27.5m in March 2000 from nine million a year before (Soteriou and Zenios, 2003). In September 2012, online desktop banking reached 70% of UK Internet users, up from 63% in October 2011 (eMarketer, 2013). In June 2014 the RBS has announced a $1.7 bn investment into its online banking program (LSE, 2014). New banks such as Egg and First Direct entered the market in the late 1990s triggering the industry to develop new products, services and distribution channels for their ever increasingly computer savvy customers.

Electronic banking, known as e-banking, has expanded from just providing cashpoint (automated teller machines) and automated bill payments in the mid-1990s to include online services such as electronic payments, computer banking, account opening and borrowing facilities (Kolodinsky et al., 2004). Banks by their very nature need to manage risks in the following typical areas: strategic, credit, market, liquidity, operational, compliance/legal/regulatory and reputation (Georgescu, 2006). However, following the introduction and growth of e-banking, the industry has become exposed to even greater challenges from risks relating to operation, security, legal and reputational risk management which if ignored will lead to financial losses and falling consumer confidence. Of these risks the most important is security risk because if customers do not trust the systems the banks have implemented for e-banking they will simply not use them.

The risk management practices that are used in e-banking are usually classified into board and management oversight, security controls and legal and reputational risk management, as identified by the Basel Committee on Banking Supervision (BCBS), with the underlying principles originally formulated by the Bank of International Settlements (BIS). These principles are included in a report to "help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities" (Basel, 2003, p. 5). The main aims of this paper are to investigate the risks that accompany the use of e-banking in the UK, the effects these risks can have on the bank and on their customers (from the bankers' perspective) and the way these risks are managed by the bank. The paper is organized as follows: Section 1 reviews the relevant literature, Section 2 discusses the research methodology, Section 3 explains the results and the final section concludes the research and suggests areas for future research.

1. Review of the relevant literature

We review the e-banking literature that examines the challenges (including technology) and risk management procedures for banks that have adopted e-banking practices which provide the basis for the research rationale.

1.1. Challenges and issues in e-banking. E-banking research has uncovered a number of challenges facing the industry; the most significant is identified by Titrade et al. (2008, p. 1540) who stated "Security is one

of the most discussed issues around e-banking. E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments". These increased security risks can be linked to four main technological issues that must be addressed to enable a range of banking transactions to be effective and secure. Yang (1997) identifies these as security, anonymity, authentication and divisibility. The security risk posed by unauthorized access to on-line banking accounts represents a real hazard to both bank and customer in its potential to undermine confidence and confidentiality.

Security risks at the operational level include error or fraud, system disruptions or other unanticipated events resulting in the institution's inability to deliver their products or services (Mihalcescu et al., 2008). E-banking needs to increase the complexity/effectiveness of the processes and supporting technological infrastructure whilst ensuring significant controls are capable of minimizing these risks. According to Florina et al. (2008) e-banking service providers must assume a higher level of compliance risk because of the rapidly changing nature of the technology, the amount of errors that can be replicated and the frequency of regulatory changes which address e-banking issues. E-banking, similar to traditional banking, must focus on the quality, speed and reliability of its service, as Furst et al. (2000) suggest many e-businesses failed in the earlier dot.com era because of this. Customers' faith in using technology also needs consideration as Yang et al. (2007) highlight the lack of familiarity or confidence with the Internet, prominent among senior citizens, makes some customers reluctant to trust doing their banking online. Kumar et al. (2012) state that the lower level of adoption of e-banking is linked to the level of trust. Despite conceding that the engagement with Internet banking is positively related with levels of different types of trust they say that the means to develop such trust is still not clearly known.

1.2. Risk management in e-banking. All organizations conducting their business on-line have to focus on controlling the associated risks; e-banking is no exception. Malisuwan (2006) categorizes these e-banking risks into three main areas to be managed: Board and Management Oversight, Security Controls and Legal and Reputational Risk Management based on the fourteen "risk management principles" identified by the Electronic Banking Group (EBG) of the BCBS. Georgescu (2006) suggests that the competitive pressure to launch new innovative products in very short time scales intensifies the management challenge to ensure that adequate strategic assessment, risk analysis and security reviews are undertaken.

Strategic risk: Kondabagil (2007) suggests that strategic risk applies to all aspects of banking but is specific to e-banking when the management does not adequately plan, manage or monitor the performance of the different electronic banking channels. These risks need minimizing by implementing an effective IT corporate governance program to oversee the formation of strategies, management of processes, performance and risk measurement of the institution's e-banking. Khan and Karim (1997) suggest that the Bank's board and management should be responsible for understanding and evaluating the strategic risks of e-banking and comparing the risk management costs against the potential return on the investment. Particular attention should be paid to the adequacy of management information systems to track usage, cost and profitability, competition from other banking providers and adequacy of technical, operational, compliance or marketing support for e-banking products and services.

Operational/transaction risk: Complex rapidly changing technological advances and the introduction of explicit capital adequacy requirements under the Basel II accord in 2006 are two key factors that have focused on operational risk. Traditional banking management processes have concentrated on market, credit and security risks but there are not many established frameworks for operational risk in e-banking. Kondabagil (2007) argues that reducing operational risks is dependent upon having direct and active risk controls. A number of e-banking facilities could be considered for outsourcing but Ramakrishnan (2001) recommends that third party providers should be limited because of the increased transaction risks resulting from the lack of continuity of control over the processes and systems used. Khan and Karim (1997) suggest that the key to controlling operational risk lies in having effective policies, procedures and controls to meet these new risks. Furthermore it is argued by Titrade et al. (2008) that segregation of duties, dual control and reconcilements remain important internal controls as information security controls become more significant. The level of controls needed should be linked to the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level. Anghelache et al. (2011) highlight the implementation of operational risk issues and suggest that financial institutions should identify, plan and avoid operational risk by using advanced methods of operational risk management.

Legal/compliance risk: E-banking product and service providers face a high level of compliance risk as a result of the ever evolving legal and regulatory changes often resulting from the rapid pace of technological changes. Failure to comply with these changes often has serious consequences involving rating downgrades, regulatory enforcement action, monetary fines, suspension of operations, reputational damage and even withdrawal of authorisation to

operate (Kondabagil, 2007). Typical legal issues relating to customer privacy and disclosure must be managed at the basic level as well as contending with more serious situations involving money laundering resulting from systems that offer liberal balance and transaction limits and limited authentication of transactions (Pennathur, 2001). E-banking transactions are often conducted remotely which makes it increasingly difficult to apply traditional methods of detecting and preventing the money launderer's activity (Shirazi, 2003). Compliance risks are often compounded in cross border situations as conflicting laws, tax procedures and reporting requirements add to the risk (Ramakrishnan, 2001). E-banking needs a responsibly managed compliance function employing well trained up-todate personnel and the strengthening of risk mitigation measures to help reduce these risks (Kondabagil, 2007).

Reputational risk: Difficulties resulting from security or legal issues can impact on the reputation of a bank ranging from dissatisfaction with online services to security breaches and fraud (Pennathur, 2001). One of the biggest issues in e-banking is "phishing", the act of acquiring private or sensitive data for use in fraudulent activities, which can lead to an irreparable loss of trust between the customer and the bank. Reputational risk impairs the bank's ability to establish and maintain customer relationships which can also be systematic. Substantial loss caused by the mistakes or disruptions of other banks, offering similar e-banking, may cause customers to be sceptical as it can impact on the reputation of all banks (Shirazi, 2003; Sokolov, 2007). The key for banks is to manage and control this risk, as Kondabagil (2007) notes, customer education along with formal incident response and management procedures can show that the benefits customers gain from the service outweigh the potential risks.

2. Research methodology

Initially a semistructured interview is conducted as a pilot study with four suitably knowledgeable and experienced key staff members of one of the leading UK banks, to examine the employee's views on risk management issues for e-banking. Following the pilot study a questionnaire is developed and used across ten major UK banks to establish whether they are operating in line with the underlying risk management principles. A similar approach was undertaken by Sokolov (2007) who used the risk management principles identified by the Basel Committee on Banking Supervision (BCBS) under the three key headings of board and management oversight, security controls and legal and reputational risk management.

Interviews: The semistructured interviews cover the following eight questions.

Q_1. What benefits do you believe electronic banking brings to customers of the bank?
Q_2. What do you believe the main risks that affect customers using electronic banking products?
Q_3. Is there a common understanding of risk management across the bank?
Q_4. How does the bank mitigate the various risks associated with electronic banking?
Q_5. Do you believe the use of risk management techniques reduce costs or expected losses?
Q_6. Are the banks' risk management procedures/processes documented for staff to manage risks?
Q_7. What do you believe are the main risks that the bank faces from offering electronic banking?
Q_8. Has the bank been successful in managing the risks they face from electronic banking?

Questionnaire: The questionnaire is divided into three sections and addressed to the banks' e-banking specialists. Section 1 asks questions regarding three of the risk management principles relating to board management and oversight; Section 2 covers seven principles relating to security controls and Section 3 covers four principles relating to legal and reputational risk management. Each of the 14 principles requires the respondents to indicate their degree of agreement using a five level Likert scale (ranging from 1 = strongly disagree; 5 = strongly agree).

The 14 Risk management principles for electronic banking are stated below.

Board management and oversight:

- The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.
- The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.
- The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

Security controls:

- Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the Internet.
- Banks should use transaction authentication methods that promote non repudiation and establish accountability for e-banking transactions.

- Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
- Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.
- Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.
- Banks should ensure that clear audit trails exist for all e-banking transactions.
- Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

Legal and reputational risk management:

- Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e- banking transactions.
- Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.
- Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.
- Banks should develop 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.

From the original submission of 150 questionnaires 110, an initial response rate of 73.3%, have been received in which details are shown in Table 1.

Table 1. Response rates details

	Percentage distribution of respondents		
Bank name	Sent	Received	Percentage %
RBS	15	15	100.0
NatWest	15	14	93.3
The Cooperative bank	15	6	40.0
Barclays	15	14	93.3
HBOS	15	9	60.0
Santander	15	8	53.3
HSBC	15	12	80.0
Nationwide	15	10	66.7
Lloyds	15	10	66.7
Alliance and leicester	15	12	80.0
Total	150	110	73.3

After screening these responses, only 93 questionnaires are used in this paper due to incomplete data/information being provided. The information collected from analyzing the questionnaires provides some interesting results which are described in the following section.

3. Results and discussion

3.1. Interview (pilot study). The four interview participants are all involved in e-banking and all work in different departments in one of the major high street banks in the UK. They are well educated to a professional standard which allows them to answer the interview questions. The answers are analyzed to identify their views on risk management in e-banking. Table 2 provides further information on the characteristics of the four participants.

Table 2. Characteristics of participants

Participant	Role	Duration
A (male)	Risk IT business	2 years
B (male)	Group security & Fraud	1 year 6 months
C (male)	Electronic banking	5 years
D (female)	Faster payments and *E*-vision	2 years

Of the four participants who are interviewed, one is a team manager and one is a deputy manager. Many of the responses are similar which suggests there is a strong culture and loyalty within the organization which aligns to the views of Denison and Mishra (1995) who argue that when qualities such as shared beliefs and loyalty are shown by employees of an organization it can help such an organization to become more profitable. The following is a summary of the four participants' responses (a full set of their answers is provided in Appendix A).

Participant A strongly believes that there is a good understanding of risk management amongst the staff in their department as they complete quarterly exercises to ensure they are kept up-to-date. This participant believes that the risk management techniques operated at the bank definitely help reduce cost or expected loss. All current risk management procedures are documented in employee handbooks to ensure the staff are familiar with the practices and read quarterly for internal audit and compliance purposes. He believes that security risk is the most significant risk faced by the bank. *Participant B* appears to be the least experienced. His responses are more customer-focused. He stated that audit meetings are used in the department to keep staff up-to-date. This participant suggests that for the risk management techniques to be successful the customer has to be more proactive regarding the potential risks they might face. He believes that "*unauthorized access to customers' accounts*" is the most significant risk which is related to security risk.

Participant C's responses demonstrate a very experienced understanding of risk management for e-banking. He suggests that to mitigate risks the bank uses both sophisticated IT systems and staff training programs which protect them from any potential fraudsters and to ensure that all staff have a common understanding of the risk management processes. He believes that the bank's risk management techniques have helped reduce bank losses from fraudulent activities, and interestingly the bank coordinates with other organizations to help tackle these risks. The participant takes a different view regarding the most significant risk by suggesting that the problem is in its cost. *Participant D* gives a thorough and balanced view of the way the bank operates its risk management but is more focused on the customer when quizzed on the risks from e-banking. She suggests that breaches in the bank systems will cause a very significant risk but feels that there have not been any significant past infringements, therefore the success of the risk management systems must be appreciated. The participant highlights the most significant risk banks face is "*Vulnerability to fraud or security breaches*" which derives from the security risk category. These findings are confirmed by the Deutsch Bank research (2006).

In the first question all of the participants mentioned various benefits but Participant C is full of praise for e-banking suggesting it is a safer way to bank and customers will feel confident banking online knowing their finances are protected. This view does contrast somewhat to the fact that hackers and phishing are seemingly more prevalent over the last decade. From the second question participants A, B and D all explain that security risk is the most likely threat to e-banking customers by exposing them to fraud from methods such as phishing, emails and Malware or viruses. However from a slightly different angle participant C believes that the lack of customer education, when using e-banking services, is the biggest problem as they are unaware of the methods available to protect themselves from these potential threats.

In addition, from the fourth question participants B and C highlight how the bank informs its e-banking customers of any potential threats by using email or information boxes when they use their Internet banking. This indicates that as the bank is very proactive this enhances its reputation. Participant A suggests that the bank decreases any potential risks by having security systems in place as they help identify any risk before they become serious issues. However, this is not always possible as some security risks can spread very quickly and cannot be nullified immediately in all situations. Participant C supports participant A's view regarding the process of continually updating the IT systems which helps to keep the bank ahead of any potential innovations fraudsters have. This would appear to be in contrast to expert opinion that updating software with various fixes and patches merely catches up with the fraudsters (see for example Acohido and Swartz, 2008). Finally from the seventh question, participants A, B and D suggest that security risk is the most significant. Participants A and B add that reputational risks are significant. We believe that reputational risks cause a number of issues for the bank particularly with customer satisfaction and trust issues.

Questionnaire: The following is a discussion of the 14 principles, analyzed separately, from the respondents' perspective and shown in Tables 3 and 4.

3.2. Board and management oversight. *Principle 1: effective management oversight of e-banking activities*. 38% of the respondents strongly agree with the principle, 43% agree with only 3% disagreeing, whilst 16% are neutral. We believe this indicates that the UK banks are vigilant with their controls and policies to manage these risks. Furthermore it suggests that UK banks act responsibly in the development of business strategy and the creation of effective management oversight of risks.

Principle 2: establishment of a comprehensive security control process. 32% of the respondents strongly agree with the principle, 56% agree with 1% disagreeing and 11% are neutral. This suggests that the security control process systems in place help safeguard the banks' e-banking systems from external as well as internal threats.

Table 3. Descriptive statistics

	N	Mean	Std. Dev.	Minimum	Maximum
Board & management oversight					
$Principle_1$	93	4.1720	.77493	2.00	5.00
$Principle_2$	93	4.2151	.62292	3.00	5.00
$Principle_3$	93	3.9140	.80293	2.00	5.00
Security controls					
$Principle_4$	93	4.7849	.65689	2.00	5.00
$Principle_5$	93	4.3333	.66485	2.00	5.00
$Principle_6$	93	4.1398	.85455	2.00	5.00
$Principle_7$	93	4.6774	.53490	2.00	5.00
$Principle_8$	93	4.8495	.35954	4.00	5.00
$Principle_9$	93	4.4409	.52050	3.00	5.00
$Principle_{10}$	93	4.8495	.35954	4.00	5.00
Legal & reputational risk management					
$Principle_{11}$	93	4.8817	.32469	4.00	5.00
$Principle_{12}$	93	4.3548	.78913	2.00	5.00
$Principle_{13}$	93	4.6022	.66168	2.00	5.00
$Principle_{14}$	93	4.7742	.42038	4.00	5.00

Note: $Principle_1$ refers to effective management oversight of e-banking activities; $Principle_2$ refers to establishment of a comprehensive security control process; $Principle_3$ refers to comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies; $Principle_4$ refers to authentication of e-banking customers; $Principle_5$ refers to non-repudiation and accountability for e-banking transactions; $Principle_6$ refers to appropriate measures to ensure segregation of duties; $Principle_7$ refers to proper authorization controls within e-banking systems, databases and applications; $Principle_8$ refers to data integrity of e-banking transactions, records, and information; $Principle_9$ refers to establishment of clear audit trails for e-banking transactions; $Principle_{10}$ refers to confidentiality of key bank information; $Principle_{11}$ refers to appropriate disclosures for e-banking services; $Principle_{12}$ refers to privacy of customer information; $Principle_{13}$ refers to capacity, business continuity and contingency planning to ensure availability of e-banking systems and services; $Principle_{14}$ refers to incident response planning.

Principle 3: comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies. 22% of the respondents strongly agree with the principle, 56% agree, 6% disagree and 16% are neutral. In this section there is a higher disagreement factor when compared with the other principles. However, this remains a small proportion, so we are of the opinion that the banks have a comprehensive and ongoing evaluation system for their third parties and outsourcing relationships.

The mean for each of these principles (see Table 3) is 4.17, 4.22 and 3.91, respectively, which supports the view given that UK banks show a high level of existing risk oversight policies for their e-banking activities. The mean for principle 3 is the lowest in this section which may reflect the fact that some of the respondents may not have a full appreciation of their bank's 3rd party arrangements. Both principles 1 and 3 do have the highest neutral responses at 16% which may reflect the fact these areas could be a more specialized area than the respondents normally are involved with.

3.3. Security controls. *Principle 4: authentication of e-banking customers*. 88% of the respondents strongly agree with this principle (the joint highest response to the 14 principles), 6% agree, 3% disagree with another 3% being neutral. We are therefore, of the opinion that the UK banks are compliant with this aspect, as would be expected, as it is one of the traditional measures to implement. Unfortunately some of these measures by their very nature, simpler and/or cheaper, are still breached if the client either shares or does not keep these measures, such as passwords, confidential.

Principle 5: non-repudiation and accountability. 43% of the respondents strongly agree with the principle, 48% agree, 1% disagreeing and 8% being neutral. This indicates that their bank adheres to this security control which suggests all parties involved in the transaction are positively authenticated and a level of control is always in place.

Principle 6: segregation of duties within systems, databases and applications. 38% of the respondents strongly agree with this principle, 45% agree, a surprising 6% who disagreed and 11% who are neutral. We are of the opinion that this should be another of the areas that the bank would be able to exercise full and careful controls with regular compliance testing managed through the internal audit measures that all banks use to satisfy the external auditors for the annual reporting process. Interestingly the 6% may imply that their banks do not have the necessary controls required to maintain segregation of duties which may reflect the continual reduction of staff seen after downsizing measures.

Principle 7: authorization controls within e-banking systems, databases and applications. 70% of the respondents strongly agree with the principle and 29% agree leaving only 1% who disagrees. We are of the opinion that this should be another of the areas that the bank exercises full and careful controls ensuring individuals cannot change their status thereby gaining access to e-banking systems and databases which they should not have access to.

Principle 8: data integrity of e-banking transactions, records, *and information*. 85% of the respondents strongly agree with this principle and 15% agree. This is one of the most positive responses in the survey. This suggests that their e-banking records are stored in such a way that makes them unlikely to be modified; if the records are tampered with it is detected by transaction processing, batch controls and monitoring of exception reports.

Principle 9: establishment of clear audit trails for e-banking transactions. 45% of the respondents strongly agree with the principle and 54% agree with only 1% is neutral. With 99% being in overall agreement does not come as any real surprise to us but it is interesting the strength of agreement is not as positive as we had expected. The results suggest however that the banks do maintain clear audit trails which would be able to be confirmed from the results of their internal audit procedures.

Principle 10: confidentiality of key bank information. 85% of the respondents strongly agree with this principle and 15% agree. Similar to principle 9 the overall level of agreement is as expected but the strength of agreement is the 3rd highest of the survey. Confidentiality is an important issue with regards to risk management and underpins all banking relationships; the implications of failure include potential exposure to both reputation and legal risk. These results suggest that key information/data is being kept secure and only available to authorized and authenticated individuals.

Security controls are clearly an extremely important issue in e-banking and it is essential for banks to ensure they have established authorization and authentication measures, identifying the customer wishing to use e-banking services. From Table 3 we can observe that the mean values for each of these principles in this section range from 4.1398 (lowest – principle 6) to 4.8495 (highest – principles 8 and 10). This supports the view that the UK banks show a high level of existing security controls for their e-banking activities.

If however the banks lose their focus on this key area and fail to authenticate their customers, resulting in unauthorized access; the financial and reputational costs due to fraud and disclosure of confidential information would be catastrophic. Which is why we believe one of the most important principles is the ability for the bank to maintain data integrity of e-banking transactions (Basel committee, 2003).

3.4. Legal and reputational risk management. *Principle 11*: *appropriate disclosures for e-banking services*. 88% of the respondents strongly agree with this principle and 12% agree. With no neutrality or disagreement from the survey this is the most positive of the responses from this section and clearly indicates that these UK banks are trying to minimize any legal and reputational risk that comes from disclosures relating to their e-banking activities. We can demonstrate this further by being able to easily find 'whistleblowing' facilities for all of UK banks used in this study. Typically on-line they provide such information as the name and location of their head office and the methods by which customers can contact the bank regarding issues such as suspected fraud or complaints.

Principle 12: privacy of customer information. 48% of the respondents strongly agree with the principle and 46% agree. 6% however disagreed which is again surprising as maintaining a customer's information privacy is a key responsibility for any bank. Failures in this aspect are likely to have severe financial consequences resulting from both legal and reputational risks. Many financial institutions, including these banks, adopt the usual approach allowing customers to opt out of sharing their information with third parties for marketing purposes.

Principle 13: capacity, business continuity and contingency planning to ensure availability of e-banking systems and services. 67% of the respondents strongly agree with this principle, 30% agree and 3% disagree. This supports the view that UK banks have a planning process in place to ensure the availability of risk management systems and services. Many of the banks have dedicated duplicate computer control centres that are run in parallel so that if the mainframe fails or is disrupted then the duplicate supporting system immediately takes over. However the number of reported occasions where on-line payment systems have failed could indicate this is an area that requires further investigation.

Principle 14: incident response planning. 77% of the respondents strongly agree with the principle and 23% agree. This is another very positive response from which we can conclude that these UK banks are well prepared for any unexpected attacks on their e-banking services. We believe effective incident response systems are essential to help minimize operational, legal and reputational risks that might occur.

Table 4. Statistics related to the 14 Basel principles

	Responses										Chi² test	
	Strongly agree	%	Agree	%	Neutral	%	Disagree	%	Strongly disagree	%	DF	Sig.
Board & management oversight												
$Principle_1$	35	38	40	43	15	16	3	3	0	0	3	.000
$Principle_2$	30	32	52	56	10	11	1	1	0	0	2	.000
$Principle_3$	20	22	52	56	15	16	6	6	0	0	3	.000
Security controls												
$Principle_4$	82	88	5	6	3	3	3	3	0	0	3	.000
$Principle_5$	40	43	45	48	7	8	1	1	0	0	3	.000
$Principle_6$	35	38	42	45	10	11	6	6	0	0	3	.000
$Principle_7$	65	70	27	29	0	0	1	1	0	0	2	.000
$Principle_8$	79	85	14	15	0	0	0	0	0	0	1	.000
$Principle_9$	42	45	50	54	1	1	0	0	0	0	2	.000
$Principle_{10}$	79	85	14	15	0	0	0	0	0	0	1	.000
Legal & reputational risk management												
$Principle_{11}$	82	88	11	12	0	0	0	0	0	0	1	.000
$Principle_{12}$	45	48	43	46	0	0	5	6	0	0	2	.000
$Principle_{13}$	62	67	28	30	0	0	3	3	0	0	2	.000
$Principle_{14}$	72	77	21	23	0	0	0	0	0	0	1	.000

Note*:* $Principle_1$ refers to effective management oversight of e-banking activities, $Principle_2$ refers to establishment of a comprehensive security control process; $Principle_3$ refers to comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies; $Principle_4$ refers to authentication of e-banking customers; $Principle_5$ refers to non-repudiation and accountability for e-banking transactions; $Principle_6$ refers to appropriate measures to ensure segregation of duties; $Principle_7$ refers to proper authorization controls within e-banking systems, databases and applications; $Principle_8$ refers to data integrity of e-banking transactions, records and information; $Principle_9$ refers to establishment of clear audit trails for e-banking transactions; $Principle_{10}$ refers to confidentiality of key bank information; $Principle_{11}$ refers to appropriate disclosures for e-banking services; $Principle_{12}$ refers to privacy of customer information; $Principle_{13}$ refers to capacity, business continuity and contingency planning to ensure availability of e-banking systems and services; $Principle_{14}$ refers to incident response planning.

This section's mean values range from 4.3548 (principle 12) to 4.8817 (principle 11 – overall highest value) which when combined with the fewest neutral and disagree responses (principles 11 and 12 had neither) does indicate that these UK banks are all focussed on the key area of legal and reputational risk management. Finally, the Chi^2 test shows that there are statistically significant differences at the 99% confidence level between various respondents' responses in relation to each of the 14 principles, as shown in Table 4.

Based on the responses we have received to our pilot study and questionnaire we agree that the level of development of risk management in e-banking for these UK banks is positive. With each risk management principle the respondents have reflected upon how their bank was performing. However it should be noted that the response rate from the different banks varies considerably with three banks falling below a 2/3rds response rate, and one of these being as low as 40%. Interestingly it could be argued that this correlates to the recent corporate governance failures reported and fully discussed at Parliamentary Select Committee level (FTAdviser, 2014).

Conclusion

During the last couple of decades e-banking has become an important and growing area of interest. Risks associated with e-banking during such a period of significant growth require effective risk management processes. Based on our research findings security risks are clearly identified, as being most important, which is confirmed by the Deutsch Bank research (2006), in addition reputational risks are also considered. Having analyzed the views of the respondents it appears that UK banks are doing their utmost to manage the potential risks of e-banking and there is a common appreciation of the practices across all of the banks.

The views obtained from the semistructured interviews, used as a pilot study, confirms the results we have gained from the questionnaire responses. These results suggest the banks are working hard to mitigate the various risks and on the whole have been successful in managing the risks that accompany the use of e-banking services. This is very encouraging and does suggest that a degree of comfort may well be taken from the employees' views about the banks. However it is clear to us that they cannot afford to become complacent when considering the adverse impact of increasing customer complaints, financial ombudsman data, news headlines, corporate governance issues and credit crunch fall out which are all potentially critical of their risk control measures.

Future research could focus upon comparisons between the various banking products, delivery methods

(computer, telephone and smart technology) and their risks. This may provide subtle differences and establish whether the bank adjusts the management techniques used from product to product using different delivery methods. Our research could be expanded to cover all UK banks to investigate whether there are differences in the performance of major and minor banks; local and foreign banks; established traditional and non-traditional banks. Finally it would be interesting to consider whether the views of e-banking customers are different.

References

1. Acohido, P. & Swartz, J. (2008). "Zero day Threat: The Shocking Truth of how Banks and credit Bureaus help cyber crooks Steal Your money and identity", Google Book.
2. Anghelache, G-V., Cozmanca, B-O., Handoreanu, C-A., Obreja, C., Olteanu, A-C. & Radu, A-N. (2011). 'Operational risk – an assessment at international level', *International Journal of Mathematical Models and Methods in Applied Sciences*, 1 (5), pp. 184-192.
3. Basel Committee on Banking Supervision (2003). Risk management principles for electronic banking and electronic money activities, Bank for international settlements. Basel. Available at: http://www.bis.org/publ/bcbs98.pdf accessed on 12/03/2010.
4. Denison, D.R. and Mishra, A.K. (1995). Towards a theory of organizational culture and effectiveness. *Organization Science*, 6, pp. 204-223.
5. Deutsche Bank Research. (2006). Online Banking: What We Learn from the Differences in Europe. Available at: http: //www.dbresearch.com/PROD/DBR_MOBILE_EN-PROD/PROD0000000000196129.pdf accessed on 04/04/10.
6. eMarketer (2013). Online Banking in the UK Trumps In-Person, with More Users, More Often. Available at: http://www.emarketer.com/Article/Online-banking-UK-Trumps-In-Person-with-More-Users-More-Often/1009678 (Accessed May 2014).
7. Florina, V., Liliana, M. and Viorica, I. (2008). Risk Management of E-banking Activities. Available at http://steconomice.uoradea.ro/anale/volume/2008/v3-finances-banks-accountancy/160.pdf accessed on 04/02/10.
8. FTAdviser (2014). Co-op mess "no surprise" to Treasury select committee. Available at: http://www.ftadviser.com/2014/05/07/ifa-industry/companies-and-people/co-op-mess-no-surprise-to-treasury-select-committee-CRcuoJXLbU1IdSlB4ZQLoL/article.html (Accessed June 2014).
9. Furst, K. Lang, W.W. and Nolle, D. (2000). Internet banking: developments and prospects, *Working Paper 2000–9, Office of the Comptroller of the Currency*, Economic and Policy Analysis.
10. Georgescu, M. (2006). Some issues about risk management for E-banking, accepted paper series Social Science Research Network.
11. Khan, A.R. and Karim, M. (1997). *E-banking and Extended Risks: How to deal with the challenge*? Available at :http://www.ru.ac.bd/finance/images/stories/working_papers/ebanking-edited.pdf, accessed on 04/03/10.
12. Kolodinsky, J.M. Hogarth, J.M. and Hilgert, M.A. (2004). The adoption of electronic banking technologies by U.S consumers, *The International Journal of Bank Marketing*, 22 (4), pp. 238-259.
13. Kondabagil, J. (2007). Risk Management in Electronic Banking: Concepts and Best Practices, John Wiley and Sons (Asia) Pte Ltd.
14. Kumar, M., Sareen, M. & Barquissau, E. (2012). Relationship between types of trust and level of adoption of Internet banking, Problems and Perspectives in Management, 10 (1), pp. 82-92.
15. LSE (2014). UPDATE 1-RBS invests $1.7 bln in online banking, branch upgrades. Available at: http://www.lse.co.uk/ShareNews.asp?shareprice=RBS&code=nbas3x7l&headline=UPDATE_1RBS_invests_17_bln_in_online_banking_branch_upgrades (Accessed June 2014).
16. Mailsuwan, U. (2006). Principles of risk management for electronic banking, *Managing information in the Digital Economy: Issues & Solutions*, pp. 494-497.
17. Mihalcescu, C., Ciolacu, B., Pavel, F. and Titrade, C. (2008). Risk and Innovation in E-banking. Romanian Economic and Business Review, vol 3 (2), pp. 86-91.
18. Pennathur, K.A. (2001). "Clicks and Bricks" e-risk Mananagement for banks in the age of the internet, *Journal of Banking & Finance*, 25, pp. 2103-2123.
19. Ramakrishnan, G. (2001). Risk Management for internet banking, information, *Systems Control Journal*, Volume 6.
20. Shirazi, S.H. (2003). Risk profile in E-banking, The Pakistan Accountant. Available at: http://www.icap.org.pk/userfiles/file/awr-2.pdf accessed on 22/03/10.
21. Sokolov, D. (2007). *E-banking: Risk Management Practices of the Estonian Banks*, Institute of Economics at Tallinn University of Technology, 101 Kopli Street, 11712, Tallinn, Estonia.
22. Soteriou, A.C. and Zenios, S.A. (2003). *Delivering e-banking services: An emerging internet business model and a case study*, Working Paper 02-12, HERMES Centre of Excellence on Computational Finance & Economics.
23. Titrade, C., Ciolacu, P. & Pavel, F. (2008). *E-banking— Impact*, *Risks*, *Security*, Universitatea Romano Americana.
24. Yang, J., Whitefield, M. and Boehme, K. (2007). New issues and challenges facing e-banking in rural areas: an empirical study, *International Journal Electronic Finance*, Vol. 1, No 3.
25. Yang, Y. (1997). The Security of electronic banking. Available at http://csrc.nist.gov/nissc/1997/proceedings/041.pdf, accessed on 04/04/10.

Appendix A. Interviews details

Participant A

Q1. What benefits do you believe electronic banking brings to customers of the bank?

E-banking allows customers to be able to manage their accounts 24/7 and allows customers to save time when making transactions. It is also much more convenient for the majority of customers and with the different electronic channels available to customers nowadays they can be in control of their accounts whenever and wherever they are.

Q2. What do you believe the main risks that affect customers using electronic banking products?

The obvious risk is the security risk, as customers can be potentially exposed to these risks whenever they electronically access their accounts. The risk of fraud is also there as well. Privacy risk can also arise as customer home computers can get viruses which could expose them to fraud and also the risk of hackers infiltrating customer's accounts. Phishing is also another potential risk customers can face.

Q3. Is there a common understanding of risk management across the bank?

Yes, all staff members are trained on risk management and are given quarterly exercises and tests called ATL (access to learning). I know this department is well trained and all the staff understand the risk management processes.

Q4. How does the bank mitigate the various risks associated with electronic banking?

The bank has security systems in place which help to identify any potential threats that can affect customers. Customers are e-mailed when any potential threats that can affect them are identified and are warned to contact the bank if their details are in danger.

Q5. Do you believe the use of risk management techniques reduce costs or expected losses?

Yes, most defiantly as if these processes were not in place the customers and the banks would face heighted risks from potential fraud. Even though losses are still occurring the risk management techniques that are used help lower the losses that are caused by risks that accompany electronic banking.

Q6. Are the banks' risk management procedures/processes documented for staff to manage risks?

Yes, they are documented in all the employee handbooks and training is conducted on a quarterly basis.

Q7. What do you believe are the main risks that the bank faces from offering electronic banking?

Security risk is the main risk, it is broad, it covers fraud, phishing etc. Reputational risk is also important as if a bank suffers a very high profile breach of security, it will make customers be very wary of conducting transactions electronically.

Q8. Has the bank been successful in managing the risks they face from electronic banking?

Yes, there have not been any major security breaches from my knowledge and the bank is everyday working on finding ways to improve their processes.

Participant B

Q1. What benefits do you believe electronic banking brings to customers of the bank?

I feel that it gives customers a new way of accessing their details. It's a quick and easy way of viewing information without the need to deal with a bank physically.

Q2. What do you believe the main risks that affect customers using electronic banking products?

I think the main risks involved are with the unauthorized entry into one's account. For example if someone has malware or a virus on their pc that records information such as login details and account details this could lead to a potential breach that could result in fraud.

Q3. Is there a common understanding of risk management across the bank?

Yes, there is. As all parts of the bank liaise with each other and we have regular audit meetings assess and controls that are in place to make sure that these controls are working.

Q4. How does the bank mitigate the various risks associated with electronic banking?

We make sure that each customer is fully advised of any the potential risks that occur. We also tell each customer to take precautions as with any thing and to make sure they don't give out all their personal information online because this is something we would never ask a customer for.

Q5. Do you believe the use of risk management techniques reduce costs or expected losses?

To a certain extent I believe this works but with any system it's only as good and secure as the people who use it. This means if we have customers who aren't fully aware of the implications of actions they undertake when using electronic banking and they allow the system to be compromised then the system will appear to be incapable of functioning properly. So to summarize, I do believe that the techniques in place do work and with good training it can help reduce any potential losses.

Q6. Are the banks' risk management procedures/processes documented for staff to manage risks?

Yes they are documented both electronically and a hard copy is also available for staff to view at any time they choose.

Q7. What do you believe are the main risks that the bank faces from offering electronic banking?

I believe the most significant risk that the bank faces is unauthorized access to a customer's accounts and thereby using the funds of a customer without the customer's knowledge and the bank will be liable for this.

Q8. Has the bank been successful in managing the risks they face from electronic banking?

Yes the bank has been successful in its management of potential risks that they face. We use different tools to make sure that we are up to date with all the possible threats and take appropriate action to make sure that we protect our customers.

Participant C

Q1. What benefits do you believe electronic banking brings to customers of the bank?

Electronic banking in the 21st century is excellent for the era of electronic transactions i.e. internet transactions, phone transactions, POS transactions etcetera. It serves as the minimum security provision to customers who are otherwise vulnerable to circling sharks (fraudsters). The benefits also include the enhancement of consumer confidence whilst shopping using any medium and customer protection from the unnecessary burden of having to deal loss of finances.

Q2. What do you believe the main risks that affect customers using electronic banking products?

The main risk of adoption is the lack of education; customers are left to navigate their ways through the process through impromptu publications. Ignorance of the full usage terms and knowledge can cause an advert effect.

Q3. Is there a common understanding of risk management across the bank?

The risk management department of the organization monitors the in-depth risk exposures to all bank clients; however other departments within the bank are trained and aware of the rudiments of the organizations' risk management protocols.

Q4. How does the bank mitigate the various risks associated with electronic banking?

The bank is on the forefront of technological risk management enhancements. The IT systems are updated very frequently to keep a few steps ahead of innovative fraudsters. The bank also invests a significant sum on the training of staff and also heightens its partnership with the serious fraud office (SFO) by sharing of information and the production of risk mitigating tools. The bank also works closely with other organizations to form a coherent risk management platform.

Q5. Do you believe the use of risk management techniques reduce costs or expected losses?

In recent years, fraud levels have reduced significantly with the introduction techniques such as the chip and pin services, online protection services etcetera. Subsequently, the bank losses due to fraudulent activities have also dropped. The cost of risk management has also reduced considerably because of the joint partnership between the bank and other banks, meaning the costs are shared.

Q6. Are the banks' risk management procedures/processes documented for staff to manage risks?

Aforementioned in my response to Q3, the necessary department have extensive training, and one would only imagine that the trainings are well documented and all staff members would posses a copy as it is a common practice within the bank.

Q7. What do you believe are the main risks that the bank faces from offering electronic banking?

The cost base is usually a cause for concern as with any similar practices, however the cost base for implementing rigorous risk mitigation techniques are shared with other banks. Financially the bank stands in good stead to maintaining an admirable cost base.

Q8. Has the bank been successful in managing the risks they face from electronic banking?

From the early days of converting to electronic banking, the organization has come a long way to increasing its risk management. The bank has steadfastly taken the necessary steps to mitigate the intrinsic risk exposures to itself and clients alike. The losses are far less than in earlier years and one would dim risk management strategy a tremendous success.

Participant D

Q1. What benefits do you believe electronic banking brings to customers of the bank?

An improved ability to manage and access money and personal bank account facilities, independent of the usual opening and closing times of an actual bank.

Q2. What do you believe the main risks that affect customers using electronic banking products?

A dependency on viable security settings and capabilities and awareness amongst customers that there are people who will attempt to violate their electronic banking privileges if used incorrectly i.e. personal access details left and stored on a public computer, phishing e-mails sent out and inadvertently accessed.

Q3. Is there a common understanding of risk management across the bank?

Customers should realize there is an increased responsibility leveraged onto them when using electronic banking facilities, on top of the natural responsibility given to the bank when managing customers money.

Q4. How does the bank mitigate the various risks associated with electronic banking?

Advertizing materials are used to promote the idea of customer awareness when using electronic banking. Such marketing helps to highlight the need for due diligence with any personal information and data that could otherwise compromise overall security.

Q5. Do you believe the use of risk management techniques reduce costs or expected losses?

They should be expected to reduce both costs and losses across the board. The adoption of electronic banking in theory saves money.

Q6. Are the banks' risk management procedures/processes documented for staff to manage risks?

Yes, I think there are many examples of when banks have provided documentation to staff, regarding the management of risk.

Q7. What do you believe are the main risks that the bank faces from offering electronic banking?

A general underlying vulnerability to fraud or security breaches drawn from subtle malware software on personal customer accounts or advanced criminal computer hacking.

Q8. Has the bank been successful in managing the risks they face from electronic banking?

To date there have been no large scale breaches of security which suggests that no major bank has yet succumbed to the efforts of computer criminal activity online. This leads me to believe that the current risks incumbent with electronic banking are at present being well managed, though vigilance and prudence is always necessary.

Appendix B. Research questionnaire

On a scale of 1 to 5, please circle your appropriate answer. 5 = strongly agree; 4 = agree; 3 = neutral; 2 = disagree; 1 = strongly disagree.

Table 1b. A Research questionnaire given to bank workers

Statement		Scale				
A. Board and management oversight (principles 1 to 3)						
1	The Board of Directors and Senior Managers have established effective Management Oversight over the risks associated with e-banking activities, including the establishment of specific policies and controls to manage these risks	5	4	3	2	1
2	The Board of Directors and Senior Managers have reviewed and approved the key aspects of the banks security control process.	5	4	3	2	1
3	The Board of Directors and senior management have established a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking	5	4	3	2	1
B. Security controls (principles 4 to 10)						
4	The Bank takes appropriate measures to authenticate the identity and authorization of customers with whom it conducts business with	5	4	3	2	1
5	The Bank uses transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions	5	4	3	2	1
6	The Bank ensures that appropriate measures are in place to promote adequate segregation of duties within e-banking systems	5	4	3	2	1
7	The Bank ensures that proper authorization controls and access privileges are in place for e-banking systems, databases and applications	5	4	3	2	1

Table 1b (cont.). A Research questionnaire given to bank workers

8	The Bank ensures that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information	5	4	3	2	1
9	There are clear audit trails for all e-banking transactions	5	4	3	2	1
10	The Bank takes appropriate measures to preserve the confidentiality of key e-banking information	5	4	3	2	1
C. Legal and reputational risk management (principles 11 to 14)						
11	The Bank ensures that adequate information is provided on their websites to allow potential customers to make an informed conclusion about their e-banking services	5	4	3	2	1
12	The Bank takes appropriate measures to ensure adherence to customer privacy requirements	5	4	3	2	1
13	The Bank has an effective capacity, business continuity and contingency planning process to help ensure the availability of e-banking services	5	4	3	2	1
14	The Bank has a developed appropriate incident response plan to manage, contain and minimize problems arising from unexpected events including internal and external attacks.	5	4	3	2	1