Risk Management Principles for

Electronic Banking

Basel Committee on Banking Supervision

Basel

May 2001

Table of Contents

Electronic Banking Group

Of the Basel Committee on Banking Supervision

Chairman:
Mr John Hawke, Jr - Comptroller of the Currency, Washington DC

Members:

Commission Bancaire et Financière, Belgium	Mr Jos Meuleman Mr Koen Algoet
Office of the Superintendent of Financial Institutions, Canada	Ms Judy Cameron Mr Brad Sullivan
Commission Bancaire, France	Mr Alain Duchâteau Mr.Jerôme Deslandes
Bundesaufsichtsamt für das Kreditwesen, Germany	Mr Stefan Czekay
Deutsche Bundesbank, Germany	Ms Magdalene Heid Mr Andi Kloefer
Banca d'Italia, Italy	Mr Filippo Siracusano
Financial Supervisory Agency, Japan	Mr Kazuo Kojima Mr Tadaaki Kawamura
Bank of Japan, Japan	Mr Toshihiko Mori Mr Hiroaki Kuwahara Ms Tomoko Suzuki
Commission de Surveillance du Secteur Financier, Luxemburg	Mr David Hagen Mr Claude Bernard
De Nederlandsche Bank N.V., The Netherlands	Mr Erik Smid
Banco de España, Spain	Ms Maria Jesús Nieto
Financial Supervisory Authority, Sweden	Mr Jan Hedqvist
Federal Banking Commission, Switzerland	Mr Daniel Schmid
Financial Services Authority, United Kingdom	Mr Jeremy Quick Ms Katy Martin
Office of the Comptroller of the Currency (OCC), United States	Mr Hugh Kelly Mr Clifford Wilke
Board of Governors of the Federal Reserve System, United States	Ms Heidi Richards Mr Jeff Marquardt

Federal Deposit Insurance Corporation, United States	Ms Sandra Thomson Mr John Carter
Federal Reserve Bank of New York, United States	Mr George Juncker Ms Barbara Yelcich Mr Christopher Calabia Mr Thomas Whitford
Secretariat, Basel Committee on Banking Supervision, Bank for International Settlements:	Mr J-P Svoronos

Observers:

Australian Prudential Regulation Authority:	Mr Graham Johnson
European Central Bank:	Mr Michael Olsen
Hong Kong Monetary Authority:	Mr Brian Lee
Monetary Authority of Singapore:	Mr Enoch Ch'ng

Executive Summary

Continuing technological innovation and competition among existing banking organisations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits.

The Basel Committee on Banking Supervision expects such risks to be recognised, addressed and managed by banking institutions in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology. While not creating inherently new risks, the Committee noted that these characteristics increased and modified some of the traditional risks associated with banking activities, in particular strategic, operational, legal and reputational risks, thereby influencing the overall risk profile of banking.

Based on these conclusions, the Committee considers that while existing risk management principles remain applicable to e-banking activities, such principles must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of e-banking activities. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. The Committee also believes that the integration of e-banking applications with legacy systems implies an integrated risk management approach for all banking activities of a banking institution.

To facilitate these developments, the Committee has identified fourteen *Risk Management Principles for Electronic Banking* to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities.

These *Risk Management Principles* are not put forth as absolute requirements or even "best practice." The Committee believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated because of the speed of change related to technological and customer service innovation. The Committee has therefore preferred to express supervisory expectations and guidance in the form of *Risk Management Principles* in order to promote safety and soundness for e-banking activities, while preserving the necessary flexibility in implementation that derives in part from the speed of change in this area. Further, the Committee recognises that each bank's risk profile is different and requires a tailored risk mitigation approach appropriate for the scale of the e-banking operations, the materiality of

the risks present, and the willingness and ability of the institution to manage these risks. This implies that a "one size fits all" approach to e-banking risk management issues may not be appropriate.

For a similar reason, the *Risk Management Principles* issued by the Committee do not attempt to set specific technical solutions or standards relating to e-banking. Technical solutions are to be addressed by institutions and standard setting bodies as technology evolves. However, this Report contains appendices that list some examples current and widespread risk mitigation practices in the e-banking area that are supportive of the *Risk Management Principles*.

Consequently, the *Risk Management Principles* and sound practices identified in this Report are expected to be used as tools by national supervisors and implemented with adaptations to reflect specific national requirements and individual risk profiles where necessary. In some areas, the Principles have been expressed by the Committee or by national supervisors in previous bank supervisory guidance. However, some issues, such as the management of outsourcing relationships, security controls and legal and reputational risk management, warrant more detailed principles than those expressed to date due to the unique characteristics and implications of the Internet distribution channel.

The *Risk Management Principles* fall into three broad, and often overlapping, categories of issues that are listed to provide clarity: *Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management*.

- ***Board and Management Oversight***

Because the Board of Directors and senior management are responsible for developing the institution's business strategy and establishing an effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. Effective management oversight is expected to encompass the review and approval of the key aspects of the bank's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. It also should include a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical e-banking functions.

- ***Security Controls***

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

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that

approaches the level they can expect when using traditional banking distribution channels. To minimise legal and reputational risk associated with e-banking activities conducted both domestically and cross-border, banks should make adequate disclosure of information on their web sites and take appropriate measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing e-banking services.

- ***Legal and Reputational Risk Management***

To protect banks against business, legal and reputation risk, e-banking services must be delivered on a consistent and timely basis in accordance with high customer expectations for constant and rapid availability and potentially high transaction demand. The bank must have the ability to deliver e-banking services to all end-users and be able to maintain such availability in all circumstances. Effective incident response mechanisms are also critical to minimise operational, legal and reputational risks arising from unexpected events, including internal and external attacks, that may affect the provision of e-banking systems and services. To meet customers' expectations, banks should therefore have effective capacity, business continuity and contingency planning. Banks should also develop appropriate incident response plans, including communication strategies, that ensure business continuity, control reputation risk and limit liability associated with disruptions in their e-banking services.

This Report on *Risk Management Principles for Electronic Banking* is being publicly released. Comments from banking organisations and bank supervisors are welcome and may be addressed to the Basel Committee on Banking Supervision by fax (+41 61 280 91 00) or e-mailed to jean-philippe.svoronos@bis.org. Comments from banking organisations should be copied to the national supervisory authorities, where appropriate.

Risk Management Principles for Electronic Banking

I. Introduction

Banking organisations have been delivering electronic services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible automated machines for currency withdrawal and retail account management, are global fixtures. However, the increased world-wide acceptance of the Internet[1] as a delivery channel for banking products and services provides new business opportunities for banks as well as service benefits for their customers.

Continuing technological innovation and competition among existing banking organisations and new market entrants has allowed for a much wider array of electronic banking[2] products and services for retail and wholesale banking customers. These include traditional activities such as accessing financial information, obtaining loans and opening deposit accounts, as well as relatively new products and services such as electronic bill payment services, personalised financial "portals," account aggregation[3] and business-to-business market places and exchanges.

Notwithstanding the significant benefits of technological innovation, the rapid development of e-banking capabilities carries risks as well as benefits and it is important that these risks are recognised and managed by banking institutions in a prudent manner.[4] These developments led the Basel Committee on Banking Supervision to conduct a preliminary study of the risk management implications of e-banking and e-money in 1998.[5] This early study demonstrated a clear need for more work in the area of e-banking risk management and that mission was entrusted to a working group comprised of bank supervisors and central banks, the Electronic Banking Group (EBG), which was formed in November 1999.

---

1 For the purposes of this Report, the Internet is defined to include all related web enabling technologies and open telecommunications networks ranging from direct dial-up connections, the public World Wide Web, and virtual private networks.

2 For the purpose of this Report, electronic banking, or ***e-banking***, includes the provision of retail and small value banking products and services through electronic channels as well as large value electronic payments and other wholesale banking services delivered electronically.

3 Account aggregation services allow customers to obtain consolidated information about their financial and non-financial accounts in one place. An aggregator essentially acts as agent for customers to provide consolidated information on customers' accounts across several financial institutions. Customers provide the aggregator with the necessary security password or personal identification number to access and consolidate account information primarily through screen scraping, a process that involves culling data from the other institutions' websites, often without their knowledge, or through contractually arranged direct data feeds between financial institutions.

4 Because of rapid changes in information technology, no description of such of risks can be exhaustive. However, the risks facing banks engaged in e-banking are generally not new and they are encompassed by risk categories identified in the Basel Committee's *Core Principles for Effective Banking Supervision*, September 1997. That guidance identified eight risk categories including credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk. The *Core Principles* are available on the BIS website at http://www.bis.org.

5 *"Risk Management for Electronic Banking and Electronic Money Activities*", March 1998, available on the Bank for International Settlements' website at http://www.bis.org.

The Basel Committee released the EBG's Report on risk management and supervisory issues arising from e-banking developments in October 2000.[6] This Report inventoried and assessed the major risks associated with e-banking, namely strategic risk, reputational risk, operational risk (including security and legal risks)[7], and credit, market, and liquidity risks. The EBG concluded that e-banking activities did not raise risks that were not already identified by the previous work of the Basel Committee. However, it noted that e-banking increase and modifies some of these traditional risks, thereby influencing the overall risk profile of banking. In particular, strategic risk, operational risk, and reputational risk are certainly heightened by the rapid introduction and underlying technological complexity of e-banking activities.

Risk Management Challenges

The EBG noted that the fundamental characteristics of e-banking (and e-commerce more generally) posed a number of risk management challenges:

- The speed of change relating to technological and customer service innovation in e-banking is unprecedented. Historically, new banking applications were implemented over relatively long periods of time and only after in-depth testing. Today, however, banks are experiencing competitive pressure to roll out new business applications in very compressed time frames – often only a few months from concept to production. This competition intensifies the management challenge to ensure that adequate strategic assessment, risk analysis and security reviews are conducted prior to implementing new e-banking applications.

- Transactional e-banking web sites and associated retail and wholesale business applications are typically integrated as much as possible with legacy computer systems to allow more straight-through processing of electronic transactions. Such straight-through automated processing reduces opportunities for human error and fraud inherent in manual processes, but it also increases dependence on sound systems design and architecture as well as system interoperability and operational scalability.

- E-banking increases banks' dependence on information technology, thereby increasing the technical complexity of many operational and security issues and furthering a trend towards more partnerships, alliances and outsourcing arrangements with third parties, many of whom are unregulated. This development has been leading to the creation of new business models involving banks and non-bank entities, such as Internet service providers, telecommunication companies and other technology firms.

- The Internet is ubiquitous and global by nature. It is an open network accessible from anywhere in the world by unknown parties, with routing of messages through unknown locations and via fast evolving wireless devices. Therefore, it significantly magnifies the importance of security controls, customer authentication techniques, data protection, audit trail procedures, and customer privacy standards.

---

6 *"Electronic Banking Group Initiatives and White Papers"*, October 2000, available on the BIS website at http://www.bis.org.

7 This Report uses the Basel Committee's Risk Management Group's definition of Operational Risk, which includes security risk and legal risk.

Risk Management Principles

Based on the early work of the EBG, the Committee concluded that, while traditional banking risk management principles are applicable to e-banking activities, the complex characteristics of the Internet delivery channel dictate that the application of these principles must be tailored to fit many online banking activities and their attendant risk management challenges. To this end, the Committee believes that it is incumbent upon the Boards of Directors and banks' senior management to take steps to ensure that their institutions have reviewed and modified where necessary their existing risk management policies and processes to cover their current or planned e-banking activities. Further, as the Committee believes that banks should adopt an integrated risk management approach for all banking activities, it is critical that the risk management oversight afforded e-banking activities becomes an integral part of the banking institution's overall risk management framework.

To facilitate these developments, the Committee asked the EBG to identify the key risk management principles that would help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities and, in turn, promote the safe and sound electronic delivery of banking products and services.

These *Risk Management Principles for Electronic Banking*, which are identified in this Report, are not put forth as absolute requirements or even "best practice" but rather as guidance to promote safe and sound e-banking activities. The Committee believes that setting detailed risk management requirements in the area of e-banking might be counter-productive, if only because these would be likely to become rapidly outdated by the speed of change related to technological and product innovation. Therefore the principles included in the present Report express supervisory expectations related to the overall objective of banking supervision to ensure safety and soundness in the financial system rather than stringent regulations.

The Committee is of the view that such supervisory expectations should be tailored and adapted to the e-banking distribution channel but not be fundamentally different to those applied to banking activities delivered through other distribution channels. Consequently, the principles presented below are largely derived and adapted from supervisory principles that have already been expressed by the Committee or national supervisors over a number of years. In some areas, such as the management of outsourcing relationships, security controls and legal and reputational risk management, the characteristics and implications of the Internet distribution channel introduce a need for more detailed principles than those expressed to date.

The Committee recognises that banks will need to develop risk management processes appropriate for their individual risk profile, operational structure and corporate governance culture, as well as in conformance with the specific risk management requirements and policies set forth by the bank supervisors in their particular jurisdiction(s). Further, the numerous e-banking risk management practices identified in this Report, while representative of current industry sound practice, should not be considered to be all-inclusive or definitive, since many security controls and other risk management techniques continue to evolve rapidly to keep pace with new technologies and business applications.

This Report does not attempt to dictate specific technical solutions to address particular risks or set technical standards relating to e-banking. Technical issues will need to be addressed on an on-going basis by both banking institutions and various standards-setting bodies as technology evolves. Further, as the industry continues to address e-banking technical issues, including security challenges, a variety of innovative and cost efficient risk management solutions are likely to emerge. These solutions are also likely to address issues related to the fact that banks differ in size, complexity and risk management culture and that jurisdictions differ in their legal and regulatory frameworks.

For these reasons, the Committee does not believe that a "one size fits all" approach to e-banking risk management is appropriate, and it encourages the exchange of good practices and standards to address the additional risk dimensions posed by the e-banking delivery channel. In keeping with this supervisory philosophy, the risk management principles and sound practices identified in this Report are expected to be used as tools by national supervisors and implemented with adaptations to reflect specific national requirements where necessary, to help promote safe and secure e-banking activities and operations.

The Committee recognises that each bank's risk profile is different and requires a risk mitigation approach appropriate for the scale of the e-banking operations, the materiality of the risks present, and the willingness and ability of the institution to manage these risks. These differences imply that the risk management principles presented in this Report are intended to be flexible enough to be implemented by all relevant institutions across jurisdictions. National supervisors will assess the materiality of the risks related to e-banking activities present at a given bank and whether, and to what extent, the risk management principles for e-banking have been adequately met by the bank's risk management framework.

II. Risk Management Principles for Electronic Banking

The e-banking risk management principles identified in this Report fall into three broad, and often overlapping, categories of issues. However, these principles are not weighted by order of preference or importance. If only because such weighting might change over time, it is preferable to remain neutral and avoid such prioritisation.

A. Board and Management Oversight [8] (Principles 1 to 3):

1. Effective management oversight of e-banking activities.

2. Establishment of a comprehensive security control process.

3. Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.

B. Security Controls (Principles 4 to 10):

4. Authentication of e-banking customers.

5. Non-repudiation and accountability for e-banking transactions.

---

[8] This Report refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its duties. For this reason it is sometimes known as the supervisory board. In such cases, the board has no executive powers. By contrast, in other countries, the board has a broader competence including the definition of the bank's general management framework. Because of these differences, the terms "board of directors" and "senior management" are used in the report to identify two decision-making functions within a bank but not to identify legal constructs.

6. Appropriate measures to ensure segregation of duties.

7. Proper authorisation controls within e-banking systems, databases and applications.

8. Data integrity of e-banking transactions, records, and information.

9. Establishment of clear audit trails for e-banking transactions.

10. Confidentiality of key bank information.

C. Legal and Reputational Risk Management (Principles 11 to 14):

11. Appropriate disclosures for e-banking services.

12. Privacy of customer information.

13. Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services.

14. Incident response planning.

Each of the above issues is discussed more specifically in the following sections, as they relate to e-banking and the underlying risk management principles that should be considered by banks to address these issues. Where appropriate, sound practices that may be considered as effective ways to address these risks are also offered in a referenced appendix.

A. Board and Management Oversight (Principles 1 to 3)

The Board of Directors and senior management are responsible for developing the banking institution's business strategy. An explicit strategic decision should be made as to whether the Board wishes the bank to provide e-banking transactional services before beginning to offer such services. Specifically, the Board should ensure that e-banking plans are clearly integrated within corporate strategic goals, a risk analysis is performed of the proposed e-banking activities, appropriate risk mitigation and monitoring processes are established for identified risks, and ongoing reviews are conducted to evaluate the results of e-banking activities against the institution's business plans and objectives.

In addition, the Board and senior management should ensure that the operational and security risk dimensions of the institution's e-banking business strategies are appropriately considered and addressed. The provision of financial services over the Internet may significantly modify and/or even increase traditional banking risks (e.g. strategic, reputational, operational, credit and liquidity risk). Steps should therefore be taken to ensure that the bank's existing risk management processes, security control processes, due diligence and oversight processes for outsourcing relationships are appropriately evaluated and modified to accommodate e-banking services.

Principle 1: 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.

Vigilant management oversight is essential for the provision of effective internal controls over e-banking activities. In addition to the specific characteristics of the Internet distribution channel discussed in the Introduction, the following aspects of e-banking may pose considerable challenge to traditional risk management processes:

- Major elements of the delivery channel (the Internet and related technologies) are outside of the bank's direct control.

- The Internet facilitates delivery of services across multiple national jurisdictions, including those not currently served by the institution through physical locations.

- The complexity of issues that are associated with e-banking and that involve highly technical language and concepts are in many cases outside the traditional experience of the Board and senior management.

In light of the unique characteristics of e-banking, new e-banking projects that may have a significant impact on the bank's risk profile and strategy should be reviewed by the Board of Directors and senior management and undergo appropriate strategic and cost/reward analysis. Without adequate up-front strategic review and ongoing performance to plan assessments, banks are at risk of underestimating the cost and/or overestimating the payback of their e-banking initiatives.

In addition, the Board and senior management should ensure that the bank does not enter into new e-banking businesses or adopt new technologies unless it has the necessary expertise to provide competent risk management oversight. Management and staff expertise should be commensurate with the technical nature and complexity of the bank's e-banking applications and underlying technologies. Adequate expertise is essential regardless of whether the bank's e-banking systems and services are managed in-house or outsourced to third parties. Senior management oversight processes should operate on a dynamic basis in order to effectively intervene and correct any material e-banking systems problems or security breaches that may occur. The increased reputational risk associated with e-banking necessitates vigilant monitoring of systems operability and customer satisfaction as well as appropriate incident reporting to the Board and senior management.

Finally, the Board and senior management should ensure that its risk management processes for its e-banking activities are integrated into the bank's overall risk management approach. The bank's existing risk management policies and processes should be evaluated to ensure that they are robust enough to cover the new risks posed by current or planned e-banking activities. Additional risk management oversight steps that the Board and senior management should consider taking include:

- Clearly establishing the banking organisation's risk appetite in relation to e-banking.

- Establishing key delegations and reporting mechanisms, including the necessary escalation procedures for incidents that impact the bank's safety, soundness or

reputation (e.g. networks penetration, employee security infractions and any serious misuse of computer facilities).[9]

- Addressing any unique risk factors associated with ensuring the security, integrity and availability of e-banking products and services, and requiring that third parties to whom the banks has outsourced key systems or applications take similar measures.

- Ensuring that appropriate due diligence and risk analysis are performed before the bank conducts cross-border e-banking activities.

The Internet greatly facilitates a bank's ability to distribute products and services over virtually unlimited geographic territory, including across national borders. Such cross-border e-banking activity, particularly if conducted without any existing licensed physical presence in the "host country," potentially subjects banks to increased legal, regulatory and country risk due to the substantial differences that may exist between jurisdictions with respect to bank licensing, supervision and customer protection requirements. Because of the need to avoid inadvertent non-compliance with a foreign country's laws or regulations, as well as to manage relevant country risk factors, banks contemplating cross-border e-banking operations need to fully explore these risks before undertaking such operations and effectively manage them.

Depending on the scope and complexity of e-banking activities, the scope and structure of risk management programs will vary across banking organisations. Resources required to oversee e-banking services should be commensurate with the transactional functionality and criticality of systems, the vulnerability of networks and the sensitivity of information being transmitted.

Principle 2: 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 oversee the development and continued maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. This should include establishing appropriate authorisation privileges, logical and physical access controls, and adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities.

Safeguarding of bank assets is one of the Board's fiduciary duties and one of senior management's fundamental responsibilities. However, it is a challenging task in a rapidly evolving e-banking environment because of the complex security risks associated with operating over the public Internet network and using innovative technology.

To ensure proper security controls for e-banking activities, the Board and senior management need to ascertain whether the bank has a comprehensive security process, including policies and procedures, that addresses potential internal and external security threats both in terms of incident prevention and response. Key elements of an effective e-banking security process include:

---

[9] In addition to internal reporting requirements, incident reporting escalation procedures should also set forth the necessary reporting to appropriate supervisory authorities.

- Assignment of explicit management/staff responsibility for overseeing the establishment and maintenance of corporate security policies.[10]

- Sufficient physical controls to prevent unauthorised physical access to the computing environment.

- Sufficient logical controls and monitoring processes[11] to prevent unauthorised internal[12] and external access to e-banking applications and databases.

- Regular review and testing of security measures and controls, including the continuous tracking of current industry security developments and installation of appropriate software upgrades, service packs and other required measures.[13]

Appendix I contain a number of additional sound practices to help ensure e-banking security.

Principle 3: 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.

Increased reliance upon partners and third party service providers to perform critical e-banking functions lessens bank management's direct control. Accordingly, a comprehensive process for managing the risks associated with outsourcing and other third-party dependencies is necessary. This process should encompass the third-party activities of partners and service providers, including the sub-contracting of outsourced activities that may have a material impact on the bank.

Historically, outsourcing was often limited to a single service provider for a given functionality. However, in recent years, banks' outsourcing relationships have increased in scale and complexity as a direct result of advances in information technology and the emergence of e-banking. Adding to the complexity is the fact that outsourced e-banking services can be sub-contracted to additional service providers and/or conducted in a foreign country. Further, as e-banking applications and services have become more technologically advanced and have grown in strategic importance, certain e-banking functional areas are dependent upon a small number of specialised third-party vendors and service providers. These developments may lead to increased risk concentrations that warrant attention both from an individual bank as well as a systemic industry standpoint.

Together, these factors underscore the need for a comprehensive and ongoing evaluation of outsourcing relationships and other external dependencies, including the associated implications for the bank's risk profile and risk management oversight abilities.[14] Board and

---

[10] This responsibility should normally not be part of the audit function, which has responsibility for seeing that the security oversight function is carried out effectively.

[11] Including controlled access rights and privileges as well as ongoing monitoring of network intrusion attempts.

[12] Including employees, contractors and those with access rights through outsourced relationships.

[13] Including measures to monitor network activity, log intrusion attempts and report of serious security breaches.

[14] Such an evaluation should also take into account the degree of control exercised on the third-party. A major shareholder in a joint venture may, in many cases, exercise more control than in the case of a contractual relationship with a service provider. However, it should not be inferred through such distinctions that shareholder control over a joint venture or a

senior management oversight of outsourcing relationships and third-party dependencies should specifically focus on ensuring that:

- The bank fully understands the risks associated with entering into an outsourcing or partnership arrangement for its e-banking systems or applications.

- An appropriate due diligence review of the competency and financial viability of any third-party service provider or partner is conducted prior to entering into any contract for e-banking services.

- The contractual accountability of all parties to the outsourcing[15] or partnership relationship is clearly defined. For instance, responsibilities for providing information to and receiving information from the service provider should be clearly defined.

- All outsourced e-banking systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards.

- Periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.

- Appropriate contingency plans for outsourced e-banking activities exist.

Appendix II lists a number of additional sound practices for managing outsourced e-banking systems and other third-party dependencies.

B. Security Controls (Principles 4 to 10)

While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking.[16] The following issues are particularly pertinent:

- Authentication

- Non-repudiation

- Data and transaction integrity

- Segregation of duties

- Authorisation controls

- Maintenance of audit trails

---

partnership will necessarily be sufficient, especially if the technologies and services necessary to operate the association are provided by the minority shareholder. Such distinctions are mainly useful to assert that evaluations should be made on a case-by-case basis.

[15] This would also include sub-contractors.

[16] For instance, where a Board relies on third-party vendors for e-banking services, it needs to ensure that the vendor has adequately addressed these issues and, at minimum, meets the bank's own standards.

- Confidentiality of key bank information

Principle 4: Banks should take appropriate measures to authenticate[17] the identity and authorisation of customers with whom it conducts business over the Internet.

It is essential in banking to confirm that a particular communication, transaction, or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions.

Customer verification during account origination is important in reducing the risk of identity theft, fraudulent account applications and money laundering. Failure on the part of the bank to adequately authenticate customers could result in unauthorised individuals gaining access to e-banking accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activity.

Establishing and authenticating an individual's identity and authorisation to access banking systems in a purely electronic open network environment can be a difficult task. Legitimate user authorisation can be misrepresented through a variety of techniques generally known as "spoofing."[18] Online hackers can also take over the session of a legitimate authorised individual through use of a "sniffer"[19] and carry out activities of a mischievous or criminal nature. Authentication control processes can in addition be circumvented through the alteration of authentication databases.

Accordingly, it is critical that banks have formal policy and procedures identifying appropriate methodology(ies) to ensure that the bank properly authenticates the identity and authorisation of an individual, agent or system [20] by means that are unique and, as far as practical, exclude unauthorised individuals or systems.[21] Banks can us a variety of methods to establish authentication, including PINs, passwords, smart cards, biometrics, and digital certificates.[22] These methods can be either single factor or multi-factor (e.g. using both a password and biometric technology[23] to authenticate). Multi-factor authentication generally provides stronger assurance.

---

[17] *Authentication* as used in this Report refers to the techniques, procedures and processes used to verify the identity and authorisation of prospective and established customers. *Identification* refers to the procedures, techniques and processes used to establish the identity of a customer when opening an account. *Authorisation* refers to the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the bank account or the authority to conduct associated transactions on that account.

[18] Spoofing is impersonating a legitimate customer through use of his/her account number, password, personal identification number (PIN) and/or email address.

[19] A sniffer is a device that is capable of eavesdropping on telecommunications traffic, capturing passwords and data in transit.

[20] Systems include the institution's own web sites.

[21] Systems must ensure that they are dealing with an authenticated individual, agent or system and with a valid authentication database.

[22] A bank may issue digital certificates using public key infrastructure (PKI) to a customer in order to secure communications with the bank. Digital certificates and PKI are discussed more fully in Principle 5.

[23] Biometric technology is an automated view of physiological or behavioural characteristics used to identify and/or authenticate a person. Common forms of biometric technology include facial scans, finger scans, iris scans, retina scans,

The bank must determine which authentication methods to use based on management's assessment of the risk posed by the e-banking system as a whole or by the various sub-components. This risk analysis should evaluate the transactional capabilities[24] of the e-banking system (e.g. funds transfer, bill payment, loan origination, account aggregation etc.), the sensitivity and value of the stored e-banking data, and the customer's ease of using the authentication method.

Robust customer identification and authentication processes are particularly important in the cross-border e-banking context given the additional difficulties that may arise from doing business electronically with customers across national borders, including the greater risk of identity impersonation and the greater difficulty in conducting effective credit checks on potential customers.

As authentication methods continue to evolve, banks are encouraged to monitor and adopt industry sound practice in this area such as ensuring that:

- Authentication databases that provide access to e-banking customer accounts or sensitive systems are protected from tampering and corruption. Any such tampering should be detectable and audit trails should be in place to document such attempts.

- Any addition, deletion or change of an individual, agent or system to an authentication database is duly authorised by an authenticated source.[25]

- Appropriate measures are in place to control the e-banking system connection such that unknown third parties cannot displace known customers.

- Authenticated e-banking sessions remain secure throughout the full duration of the session or in the event of a security lapse the session should require re-authentication.

Principle 5: Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.

Non-repudiation involves creating proof of the origin or delivery of electronic information to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent. Risk of transaction repudiation is already an issue with conventional transactions such as credit cards or securities transactions. However, e-banking heightens this risk because of the difficulties of positively authenticating the identities and authority of parties initiating transactions, the potential for altering or hijacking electronic transactions, and the potential for e-banking users to claim that transactions were fraudulently altered.

To address these heightened concerns, banks need to make reasonable efforts, commensurate with the materiality and type of the e-banking transaction, to ensure that:

---

hand scans, signature scans, voice scans and keystroke dynamics. Biometric identification systems provide very strong authentication, but may pose greater implementation complexities than other identification/authentication methods.

[24] Effective authentication measures can also reduce the risk of repudiation, in which an authorised user subsequently denies that he or she authorised a particular transaction (see also Principle 5).

[25] In some cases, the authenticated source may be an electronic source.

- E-banking systems are designed to reduce the likelihood that authorised users will initiate unintended transactions and that customers fully understand the risks associated with any transactions they initiate.

- All parties to the transaction are positively authenticated and control is maintained over the authenticated channel.

- Financial transaction data are protected from alteration and any alteration is detectable.

Banking organisations have begun to employ various techniques that help establish non-repudiation and ensure confidentiality and integrity of e-banking transactions, such as digital certificates using public key infrastructure (PKI).[26] A bank may issue a digital certificate to a customer or counterparty to allow for their unique identification/authentication and reduce the risk of transaction repudiation. Although in some countries customers' rights to disclaim transactions is provided in specific legal provisions, legislation has been passed in certain national jurisdictions making digital signatures legally enforceable. Wider global legal acceptance of such techniques is likely as technology continues to evolve.

Principle 6: Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.

Segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems and ensure that transactions and company assets are properly authorised, recorded and safeguarded. Segregation of duties is critical to ensuring the accuracy and integrity of data and is used to prevent the perpetration of fraud by an individual. If duties are adequately separated, fraud can only be committed through collusion.

E-banking services may necessitate modifying the ways in which segregation of duties are established and maintained because transactions take place over electronic systems where identities can be more readily masked or faked. In addition, operational and transaction-based functions have in many cases become more compressed and integrated in e-banking applications. Therefore, the controls traditionally required to maintain segregation of duties need to be reviewed and adapted to ensure an appropriate level of control is maintained. Because access to poorly secured databases can be more easily gained through internal or external networks, strict authorisation and identification procedures, safe and sound architecture of the straight-through processes, and adequate audit trails should be emphasised.

Common practices used to establish and maintain segregation of duties within an e-banking environment include the following:

[26] In a public key infrastructure (PKI), each party has a private/public key pair. The private key is secret so that only one person should use it. All parties use the public key. The private key generates an electronic signature on the document and the key pairs are designed so that a message encrypted with the private key can only be read by using the other key. A bank may act as its own certification authority (CA) or rely on another trusted third-party to associate a person or entity with the digital certificate. However, if a bank is to rely upon a third-party digital certificate to establish authenticity, it should confirm that the CA, when issuing the certificate, used the same level of authentication that the bank would have used to authenticate the person. The primary drawback of a PKI authentication system is that it is more complicated to implement.

- Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorise and complete a transaction.

- Segregation should be maintained between those initiating static data (including web page content) and those responsible for verifying its integrity.

- E-banking systems should be tested to ensure that segregation of duties cannot be bypassed.

- Segregation should be maintained between those developing and those administrating e-banking systems.[27]

Principle 7: Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.

In order to maintain segregation of duties, banks need to strictly control authorisation and access privileges. Failure to provide adequate authorisation control could allow individuals to alter their authority, circumvent segregation and gain access to e-banking systems, databases or applications to which they are not privileged.

In e-banking systems, the authorisations and access rights can be established in either a centralised or distributed manner within a bank and are generally stored in databases. The protection of those databases from tampering or corruption is therefore essential for effective authorisation control.

Appendix III identifies a number of sound practices to help establish proper control over authorisation and access rights to e-banking systems, databases and applications.

Principle 8: Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

Data integrity refers to the assurance that information that is in-transit or in storage is not altered without authorisation. Failure to maintain the data integrity of transactions, records and information can expose banks to financial losses as well as to substantial legal and reputational risk.

The inherent nature of straight-through processes for e-banking may make programming errors or fraudulent activities more difficult to detect at an early stage. Therefore, it is important that banks implement straight-through processing in a manner that ensures safety and soundness and data integrity.

As e-banking is transacted over public networks, transactions are exposed to the added threat of data corruption, fraud and the tampering of records. Accordingly, banks should ensure that appropriate measures are in place to ascertain the accuracy, completeness and reliability of e-banking transactions, records and information that is either transmitted over

[27] Or alternate mitigating controls should be in place.

the Internet, resident on internal bank databases, or transmitted/stored by third-party service providers on behalf of the bank.[28] Common practices used to maintain data integrity within an e-banking environment include the following:

- E-banking transactions should be conducted in a manner that makes them highly resistant to tampering throughout the entire process.
- E-banking records should be stored, accessed and modified in a manner that makes them highly resistant to tampering.
- E-banking transaction and record-keeping processes should be designed in a manner as to make it virtually impossible to circumvent detection of unauthorised changes.
- Adequate change control policies, including monitoring and testing procedures, should be in place to protect against any e-banking system changes that may erroneously or unintentionally compromise controls or data reliability.
- Any tampering with e-banking transactions or records should be detected by transaction processing, monitoring and record keeping functions.

Principle 9: Banks should ensure that clear audit trails exist for all e-banking transactions.

Delivery of financial services over the Internet can make it more difficult for banks to apply and enforce internal controls and maintain clear audit trails if these measures are not adapted to an e-banking environment. Banks are not only challenged to ensure that effective internal control can be provided in highly automated environments, but also that the controls can be independently audited, particularly for all critical e-banking events and applications.

A bank's internal control environment may be weakened if it is unable to maintain clear audit trails for its e-banking activities. This is because much, if not all, of its records and evidence supporting e-banking transactions are in an electronic format. In making a determination as to where clear audit trails should be maintained, the following types of e-banking transactions should be considered:

- The opening, modification or closing of a customer’s account.
- Any transaction with financial consequences.
- Any authorisation granted to a customer to exceed a limit.
- Any granting, modification or revocation of systems access rights or privileges.

Appendix IV identifies several sound practices to help ensure that a clear audit trail exists for e-banking transactions.

---

[28] Banks should ensure that record keeping systems are designed and installed in a manner that allows for recovery of records that may have been tampered with or degraded.

Principle 10: 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.

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

To meet these challenges concerning the preservation of confidentiality of key e-banking information, banks need to ensure that:

- All confidential bank data and records are only accessible by duly authorised and authenticated individuals, agents or systems.

- All confidential bank data are maintained in a secure manner and protected from unauthorised viewing or modification during transmission over public, private or internal networks.

- The bank's standards and controls for data use and protection must be met when third parties have access to the data through outsourcing relationships.

- All access to restricted data is logged and appropriate efforts are made to ensure that access logs are resistant to tampering.

C. Legal and Reputational Risk Management (Principles 11 to 14)

Specific customer protection and privacy regulations and laws will vary from jurisdiction to jurisdiction. However, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they would have if transacting business through traditional banking distribution channels.

Principle 11: 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.

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

Examples of such information that a bank could provide on its own website include:

- The name of the bank and the location of its head office (and local offices if applicable).

- The identity of the primary bank supervisory authority(ies) responsible for the supervision of the bank's head office.

- How customers can contact the bank's customer service centre regarding service problems, complaints, suspected misuse of accounts, etc.

- How customers can access and use applicable Ombudsman or consumer complaint schemes.

- How customers can obtain access to information on applicable national compensation or deposit insurance coverage and the level of protection that they afford (or links to websites that provide such information).

- Other information that may be appropriate or required by specific jurisdictions.[29]

Principle 12: 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.

Maintaining a customer's information privacy is a key responsibility for a bank. Misuse or unauthorised disclosure of confidential customer data exposes a bank to both legal and reputation risk. To meet these challenges concerning the preservation of privacy of customer information, banks should make reasonable endeavours to ensure that:

- The bank's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-banking products and services.

- Customers are made aware of the bank's privacy policies and relevant privacy issues concerning use of e-banking products and services.

- Customers may decline ("opt out") from permitting the bank to share with a third party for cross-marketing purposes any information about the customer's personal needs, interests, financial position or banking activity.

- Customer data are not used for purposes beyond which they are specifically allowed or for purposes beyond which customers have authorised.[30]

- The bank's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.

---

[29] For instance, the bank may wish to specify those countries in which the bank intends to provide e-banking services or, conversely, those countries in which it does not intend to provide such services.

[30] In some jurisdictions, laws and regulations may not oblige banks to seek the customer's permission to use customer data for internal purposes. However, they may oblige banks to give the customer the option to decline from permitting the bank to share such information with a third party or an affiliate. In other jurisdictions, customers may have the right to prevent the bank from using their data for either internal or external purposes.

Appendix V identifies several sound practices to help maintain the privacy of customer e-banking information.

Principle 13: Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

To protect banks against business, legal and reputation risk, e-banking services must be delivered on a consistent and timely basis in accordance with customer expectations. To achieve this, the bank must have the ability to deliver e-banking services to end-users from either primary (e.g. internal bank systems and applications) or secondary sources (e.g. systems and applications of service providers). The maintenance of adequate availability is also dependent upon the ability of contingency back-up systems to mitigate denial of service attacks or other events that may potentially cause business disruption.

The challenge to maintain continued availability of e-banking systems and applications can be considerable given the potential for high transaction demand, especially during peak time periods. In addition, high customer expectations regarding short transaction processing cycle times and constant availability (24 X 7) has also increased the importance of sound capacity, business continuity and contingency planning. To provide customers with the continuity of e-banking services that they expect, banks need to ensure that:

- Current e-banking system capacity and future scalability are analysed in light of the overall market dynamics for e-commerce and the projected rate of customer acceptance of e-banking products and services.[31]

- E-banking transaction processing capacity estimates are established, stress tested and periodically reviewed.

- Appropriate business continuity and contingency plans for critical e-banking processing and delivery systems are in place and regularly tested.

Appendix VI identifies several sound capacity, business continuity and contingency planning practices.

Principle 14: Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

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

---

[31] The current and future capacity of critical e-banking delivery systems should be assessed on an ongoing basis.

To ensure effective response to unforeseen incidents, banks should develop:

- Incident response plans to address recovery of e-banking systems and services under various scenarios, businesses and geographic locations. Scenario analysis should include consideration of the likelihood of the risk occurring and its impact on the bank. E-banking systems that are outsourced to third-party service providers should be an integral part of these plans

- Mechanisms to identify an incident or crisis as soon as it occurs, assess its materiality, and control the reputation risk associated with any disruption in service.[32]

- A communication strategy to adequately address external market and media concerns that may arise in the event of security breaches, online attacks and/or failures of e-banking systems.

- A clear process for alerting the appropriate regulatory authorities in the event of material security breaches or disruptive incidents occur.

- Incident response teams with the authority to act in an emergency and sufficiently trained in analysing incident detection/response systems and interpreting the significance of related output.

- A clear chain of command, encompassing both internal as well as outsourced operations, to ensure that prompt action is taken appropriate for the significance of the incident. In addition, escalation and internal communication procedures should be developed and include notification of the Board where appropriate.

- A process to ensure all relevant external parties, including bank customers, counterparties and the media, are informed in a timely and appropriate manner of material e-banking disruptions and business resumption developments.

- A process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents as well as to assist in the prosecution of attackers.

[32] Monitoring of help desk and customer support activities and regular review of customer complaints may help to identify gaps in information being detected and reported through established security controls versus actual intrusion activities.

Appendix I

Sound Security Control Practices for E-Banking

1. Security profiles should be created and maintained and specific authorisation privileges assigned to all users of e-banking systems and applications, including all customers, internal bank users and outsourced service providers. Logical access controls should also be designed to support proper segregation of duties.[33]

2. E-banking data and systems should be classified according to their sensitivity and importance and protected accordingly. Appropriate mechanisms, such as encryption, access control and data recovery plans should be used to protect all sensitive and high-risk e-banking systems, servers, databases and applications.

3. Storage of sensitive or high-risk data on the organisation's desktop and laptop systems should be minimised and properly protected by encryption, access control and data recovery plans.

4. Sufficient physical controls should be in place to deter unauthorised access[34] to all critical e-banking systems, servers, databases and applications.

5. Appropriate techniques should be employed to mitigate external threats to e-banking systems, including the use of:

   - Virus-scanning software at all critical entry points (e.g. remote access servers, e-mail proxy servers) and on each desktop system.

   - Intrusion detection software and other security assessment tools to periodically probe networks, servers and firewalls for weaknesses and/or violations of security policies and controls.

   - Penetration testing of internal and external networks.

6. A rigorous security review process should be applied to all employees and service providers holding sensitive positions.

---

[33] Definitions of security and quality standards and reliance on certification schemes can be institution specific or standardised (i.e. within a national banking industry in order to enhance and foster the security level of e-banking activities). Banks can also choose to establish access rights in either a centralised or distributed manner. For example, there may be a single authorisation authority responsible for assigning access rights to specific identities, groups or roles within a bank, or there may be a number of authorisation authorities established to address the varying needs within the different business lines.

[34] This should include controls guarding against unauthorised access by external parties such as visitors, contractors or technicians who may have access to the premises although they may not be directly involved in the e-banking service.

Appendix II

Sound Practices for Managing Outsourced E-Banking Systems and Services

1. Banks should adopt appropriate processes for evaluating decisions to outsource e-banking systems or services.

   - Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.

   - The decision to outsource a key e-banking function or service should be consistent with the bank's business strategies, be based on a clearly defined business need, and recognise the specific risks that outsourcing entails.

   - All affected areas of the bank need to understand how the service provider(s) will support the bank's e-banking strategy and fit into its operating structure.

2. Banks should conduct appropriate risk analysis and due diligence prior to selecting an e-banking service provider and at appropriate intervals thereafter.

   - Banks should consider developing processes for soliciting proposals from several e-banking service providers and criteria for choosing among the various proposals.

   - Once a potential service provider has been identified, the bank should conduct an appropriate due diligence review, including a risk analysis of the service provider's financial strength, reputation, risk management policies and controls, and ability to fulfil its obligations.

   - Thereafter, banks should regularly monitor and, as appropriate,[35] conduct due diligence reviews of the ability of the service provider to fulfil its service and associated risk management obligations throughout the duration of the contract.

   - Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.

   - Responsibilities for overseeing e-banking outsourcing arrangements should be clearly assigned.

---

[35] The extent of ongoing due diligence reviews should be based on the materiality of the outsourced operations and the extent of systems or risk management changes over time, including any subsequent sub-contracting the service provider may engage in.

- An appropriate exit strategy for the bank to manage risks should it need to terminate the outsourcing relationship.

3. Banks should adopt appropriate procedures for ensuring the adequacy of contracts governing e-banking. Contracts governing outsourced e-banking activities should address, for example, the following:[36]

   - The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any sub-contracting of material services are clearly defined.

   - Responsibilities for providing information to and receiving information from the service provider are clearly defined. Information from the service provider should be timely and comprehensive enough to allow the bank to adequately assess service levels and risks. Materiality thresholds and procedures to be used to notify the bank of service disruptions, security breaches and other events that pose a material risk to the bank should be spelled out.

   - Provisions that specifically address insurance coverage, the ownership of the data stored on the service provider's servers or databases, and the right of the bank to recover its data upon expiration or termination of the contract should be clearly defined.

   - Performance expectations, under both normal and contingency circumstances, are defined.

   - Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.

   - Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

   - For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.

   - The right of the bank to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans is explicitly defined.

4. Banks should ensure that periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.[37]

   - For outsourced relationships involving critical or technologically complex e-banking services/applications, banks may need to arrange for other

---

[36] As with other legal contracts that a bank may enter to, its legal counsel or legal division should review all terms and conditions in contracts governing e-banking outsourcing arrangements.

[37] Banks that do not have a specific audit function in-house should, at minimum, have staff not involved in management of outsourced relationships reviewing the effectiveness of the oversight of the outsourcing arrangement.

periodic reviews to be performed by independent third parties with sufficient technical expertise.

5. Banks should develop appropriate contingency plans for outsourced e-banking activities.

- Banks need to develop and periodically test their contingency plans for all critical e-banking systems and services that have been outsourced to third parties.

- Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.

- Banks should have an identified team that is responsible for managing recovery and assessing the financial impact of a disruption in outsourced e-banking services.

6. Banks that provide e-banking services to third parties should ensure that their operations, responsibilities, and liabilities are sufficiently clear so that serviced institutions can adequately carry out their own effective due diligence reviews and ongoing oversight of the relationship.

- Banks have a responsibility to provide serviced institutions with information necessary to identify, control and monitor any risks associated with the e-banking service arrangement.

Appendix III

Sound Authorisation Practices for E-Banking Applications

1. Specific authorisation and access privileges should be assigned to all individuals, agents or systems, which conduct e-banking activities.

2. All e-banking systems should be constructed to ensure that they interact with a valid authorisation database.

3. No individual agent or system should have the authority to change his or her own authority or access privileges in an e-banking authorisation database. [38]

4. Any addition of an individual, agent or system or changes to access privileges in an e-banking authorisation database should be duly authorised by an authenticated source empowered with the adequate authority and subject to suitable and timely oversight and audit trails.

5. Appropriate measures should be in place in order to make e-banking authorisation databases reasonably resistant to tampering. Any such tampering should be detectable through ongoing monitoring processes. Sufficient audit trails should exist to document any such tampering.

6. Any e-banking authorisation database that has been tampered with should not be used until replaced with a validated database.

7. Controls should be in place to prevent changes to authorisation levels during e-banking transaction sessions and any attempts to alter authorisation should be logged and brought to the attention of management.

[38] As this might not be feasible for system administrator users, other stringent internal controls and segregation of duties should be put in place to monitor the activities of those user accounts.

Appendix IV

Sound Audit Trail Practices for E-Banking Systems

1. Sufficient logs should be maintained for all e-banking transactions to help establish a clear audit trail and assist in dispute resolution.

2. E-banking systems should be designed and installed to capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.

3. In instances where processing systems and related audit trails are the responsibility of a third-party service provider:

    - The bank should ensure that it has access to relevant audit trails maintained by the service provider.

    - Audit trails maintained by the service provider meet the bank's standards.

Appendix V

Sound Practices to Help Maintain the Privacy of Customer E-Banking Information

1. Banks should employ appropriate cryptographic techniques, specific protocols or other security controls to ensure the confidentiality of customer e-banking data.

2. Banks should develop appropriate procedures and controls to periodically assess its customer security infrastructure and protocols for e-banking.

3. Banks should ensure that its third-party service providers have confidentiality and privacy policies that are consistent with their own.

4. Banks should take appropriate steps to inform e-banking customers about the confidentiality and privacy of their information. These steps may include:

    - Informing customers of the bank's privacy policy, possibly on the bank's website. Clear, concise language in such statements is essential to assure that the customer fully understands the privacy policy. Lengthy legal descriptions, while accurate, are likely to go unread by the majority of customers.

    - Instructing customers on the need to protect their passwords, personal identification numbers (PINs) and other banking and/or personal data.

    - Providing customers with information regarding the general security of their personal computer, including the benefits of using virus protection software, physical access controls and personal firewalls for static Internet connections.

Appendix VI

Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking

1. All e-banking services and applications, including those provided by third-party service providers, should be identified and assessed for criticality.

2. A risk assessment for each critical e-banking service and application, including the potential implications of any business disruption on the bank's credit, market, liquidity, legal, operational and reputation risk should be conducted.

3. Performance criteria for each critical e-banking service and application should be established, and service levels should be monitored against such criteria. Appropriate measures should be taken to ensure that e-banking systems can handle high and low transaction volume and that systems performance and capacity is consistent with the bank's expectations for future growth in e-banking.

4. Consideration should be given to developing processing alternatives for managing demand when e-banking systems appear to be reaching defined capacity checkpoints.

5. E-banking business continuity plans should be formulated to address any reliance on third-party service providers and any other external dependencies required achieving recovery.

6. E-banking contingency plans should set out a process for restoring or replacing e-banking processing capabilities, reconstructing supporting transaction information, and include measures to be taken to resume availability of critical e-banking systems and applications in the event of a business disruption.