BS/97/122

RISK MANAGEMENT FOR ELECTRONIC BANKING AND ELECTRONIC MONEY ACTIVITIES

Basle Committee on Banking Supervision

Basle

March 1998

Table of Contents

Risk Management for Electronic Banking and Electronic Money Activities

1. Introduction

Electronic payment media are likely to figure importantly in the development of electronic commerce, and retail electronic banking services and products, including electronic money, could provide significant new opportunities for banks. Electronic banking may allow banks to expand their markets for traditional deposit-taking and credit extension activities, and to offer new products and services or strengthen their competitive position in offering existing payment services. In addition, electronic banking could reduce operating costs for banks.

More broadly, the continued development of electronic banking and electronic money may contribute to improving the efficiency of the banking and payment system and to reducing the cost of retail transactions nationally and internationally. This could potentially result in gains in productivity and economic welfare. Consumers and merchants may be able to increase the efficiency, with which they make and receive payments, and enjoy greater convenience. Electronic banking may also increase access to the financial system for consumers who have previously found access limited.

The scope of this report is necessarily restricted in two respects. First, it deals with the risk management of electronic banking and electronic money activities from a banking supervisory perspective only and does not, for example, address the monetary consequences. Second, while many of the risks described in the report apply both to bank and non-bank issuers and providers, this report addresses banks only.

1.1. Purpose and organisation

The development and use of electronic money and some forms of electronic banking are still in their early stages. Given the degree of uncertainty about future technological and market developments in electronic banking and electronic money, it is important that supervisory authorities avoid policies that hamper useful innovation and experimentation. At the same time, the Basle Committee recognises that along with the benefits, electronic banking and electronic money activities carry risks for banking organisations, and these risks must be balanced against the benefits.

The purpose of this document is to provide considerations for supervisory authorities and banking organisations as they develop methods for identifying, assessing, managing and controlling the risks associated with electronic banking and electronic money.

The Basle Committee regards the document as an initial step in an ongoing review and discussion of supervisory issues and responses related to technological advances in electronic retail products and services.

The Basle Committee is distributing this document to supervisors worldwide with the expectation that it will facilitate development of appropriate supervisory approaches to the management of risks in electronic banking and electronic money activities. Supervisors may wish to circulate the document to the institutions under their jurisdiction.

The discussion is general in nature because the technology for electronic banking and electronic money is changing rapidly, and products and services in the future may be very different from those available today. At this relatively early stage in the development of some electronic banking and electronic money activities, many aspects of risks are neither fully discernible nor readily measurable. A premature regulatory approach would run the risk of stifling innovation and creativity in these areas. Therefore, supervisors should encourage banks to develop a risk management process rigorous and comprehensive enough to deal with known material risks, and flexible enough to accommodate changes in the type and intensity of material risks associated with their electronic banking and electronic money activities. The risk management process can be effective only if it is constantly evolving.

The remainder of this document is organised as follows. The next section of the Introduction presents definitions of electronic banking and electronic money, and refers to key roles banks can play as participants in electronic money activities. Section II identifies risks that banks may face in electronic banking and electronic money. The identification and analysis of risks does not aim to be exhaustive; rather, the discussion is intended to be illustrative of the types of problems banks may face. Among these, analysis suggests that operational, reputational, and legal risk may be more likely to arise.[1]

As the development of electronic banking and electronic money progresses, interaction between banks and their customers across national boundaries is likely to increase. Such relationships may raise different issues and risks for banks and for supervisors. In light of this, Section II includes a discussion of cross border risks.

Based on the identification and analysis of risks, Section III outlines the major steps in a risk management process for banks engaging in electronic banking and electronic

---

1 Banks are also likely to face risks that can affect the value of their shareholders' interest. For example, faced with a choice between competing new technologies, bank management risks choosing one which does not become widespread and hence may not be successful, or it may choose one which does not fit well with other products and services. As with any business decision management takes, risks to financial success posed by electronic banking and electronic money are of central concern to it and to owners. However, because supervisory authorities are charged with protecting the safety and soundness of the banking system, but not with ensuring bank profitability, such "shareholder value" issues are not of direct concern to supervisors, unless the viability of an institution is threatened. Therefore, in general, the document does not discuss this perspective on electronic money and electronic banking risks.

money activities. The process has three main steps: assessing risks, implementing measures to control risk exposures, and monitoring risks.

1.2. Definitions of electronic banking and electronic money

1.2.1 Electronic banking refers to the provision of retail and small value banking products and services through electronic channels.[2] Such products and services can include deposit-taking, lending, account management, the provision of financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money (defined separately, below).

Two fundamental aspects of electronic banking are the nature of the delivery channels through which activities are pursued, and the means for customers to gain access to those channels. Common delivery channels include "closed" and "open" networks. "Closed networks" restrict access to participants (financial institutions, consumers, merchants, and third party service providers) bound by agreements on the terms of membership. "Open networks" have no such membership requirements. Currently, widely used access devices through which electronic banking products and services can be provided to customers include point of sale terminals, automatic teller machines, telephones, personal computers, smart cards and other devices.

1.2.2 Electronic money refers to "stored value" or prepaid payment mechanisms for executing payments via point of sale terminals, direct transfers between two devices, or over open computer networks such as the Internet.[3] Stored value products include "hardware" or "card-based" mechanisms (also called "electronic purses"), and "software" or "network-based" mechanisms (also called "digital cash"). Stored value cards can be

---

2 This document focuses on retail electronic banking and electronic payment services. Large-value electronic payments and other wholesale banking services delivered electronically are outside the scope of the present discussion.

3 Several official bodies have each issued their own definition of electronic money. As pointed out in a recent Group of Ten report on electronic money, a precise definition of electronic money is difficult to provide, in part because technological innovations continue to blur distinctions between forms of prepaid electronic mechanisms. (See *Electronic Money: Consumer protection, law enforcement, supervisory and cross-border issues*, Group of Ten, April 1997, for a list of such studies.) The current document draws from both the Group of Ten report and *Security of Electronic Money*, Bank for International Settlements, August 1996, in establishing a definition of electronic money. The latter report explains distinctions in the technical representation of money on stored-value products. In particular, "balanced-based" products are devices which manipulate a numeric ledger, such that transactions are performed as debits or credits to a balance; and "note-based" products which perform transactions by transferring the appropriate amount of electronic "notes" (also called "coins" or "tokens"), which are of a fixed denomination, from one device to another. Debit cards and credit cards are retail electronic payment mechanisms, but are not considered to be electronic money because they are not prepaid mechanisms.

"single-purpose" or "multi-purpose".[4] Single-purpose cards (e.g., telephone cards) are used to purchase one type of good or service, or products from one vendor; multi-purpose cards can be used for a variety of purchases from several vendors.[5]

Banks may participate in electronic money schemes as issuers, but they may also perform other functions. Those include distributing electronic money issued by other entities; redeeming the proceeds of electronic money transactions for merchants; handling the processing, clearing, and settlement of electronic money transactions; and maintaining records of transactions.

2. Identification and analysis of risks

Because of rapid changes in information technology, no list of risks can be exhaustive. The intention in this document is to describe a broad, representative set of risks as a basis for designing general guidance for risk management. Specific risks facing banks engaged in electronic banking and electronic money activities can be grouped according to risk categories discussed in other Basle Committee risk management documents and, in this sense, the risks are not new.[6] Categorising risks in this manner can be helpful in systematically identifying risks in a banking organisation. The Annex presents examples of specific risks and problems banks may face in electronic banking and electronic money activities grouped into risk categories.

While the basic types of risks generated by electronic banking and electronic money are not new, the specific ways in which some of the risks arise, as well as the magnitude of their impact on banks, may be new for banks and supervisors. Some of the risks and problems banks may face apply both to electronic money and electronic banking activities. However, there are likely to be differences in the degree to which a particular risk is applicable across different electronic money and electronic banking activities.

---

4 Stored value cards may be characterised by the use of a magnetic stripe or a computer chip embedded in the card. A plastic card with an embedded computer chip (known as a "smart card") may perform stored value applications, in addition to other functions such as debit and credit applications.

5 Increasingly, the terms multi-purpose or multi-function are also used to convey the idea that the card or device can function as several types of payment instrument (e.g. credit card, debit card, stored value card), and/or that the card can be used for purposes besides financial transactions (e.g. identification card, repository of personal medical information). The lack of standardisation of terminology is perhaps a reflection of rapid technological innovations.

6 See, e.g., *Risk Management Guidelines for Derivatives*, Basle Committee on Banking Supervision, July 1994, and *Core Principles for Effective Banking Supervision*, Basle Committee on Banking Supervision, September 1997. The latter document includes a basic discussion of eight risk categories: credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk. *Payment Systems in the Group of Ten Countries*, Bank for International Settlements, December 1993, includes definitions of risks in banking and payment systems.

At this stage, it would appear that operational risk, reputational risk, and legal risk may be the most important risk categories for most electronic banking and electronic money activities, especially for diversified international banks, and the next three subsections discuss specific manifestations of these types of risks. Some of the specific problems cut across risk categories. For example, a breach of security allowing unauthorised access to customer information can be classified as an operational risk, but such an event also exposes the bank to legal risk and reputational risk. Even though these different types of risks may result from a single problem, appropriate risk management may require several remedies to address each of these different risks. Other risks may also be important for some forms of electronic banking and electronic money activities, and these are discussed thereafter. Possible cross border risks are also discussed.

2.1. Operational risk

Operational risk arises from the potential for loss due to significant deficiencies in system reliability or integrity. Security considerations are paramount, as banks may be subject to external or internal attacks on their systems or products. Operational risk can also arise from customer misuse, and from inadequately designed or implemented electronic banking and electronic money systems. Many of the specific possible manifestations of these risks apply to both electronic banking and electronic money.

2.1.1 Security risks

Operational risk arises with respect to the controls over access to a bank's critical accounting and risk management systems, information that it communicates with other parties and, in the case of electronic money, measures the bank uses to deter and detect counterfeiting. Controlling access to bank systems has become increasingly complex due to expanded computer capabilities, geographical dispersal of access points, and the use of various communications paths, including public networks such as the Internet. It is important to note that with electronic money, a breach of security could result in fraudulently created liabilities of the bank. For other forms of electronic banking, unauthorised access could lead to direct losses, added liabilities to customers or other problems.

A variety of specific access and authentication problems could occur. For example, inadequate controls could result in a successful attack by hackers operating via the Internet, who could access, retrieve, and use confidential customer information. In the absence of adequate controls, an outside third party could access a bank's computer system and inject a virus into it.

In addition to external attacks on electronic money and electronic banking systems, banks are exposed to operational risk with respect to employee fraud: employees

could surreptitiously acquire authentication data in order to access customer accounts, or steal stored value cards. Inadvertent errors by employees may also compromise a bank's systems.

Of direct concern to supervisory authorities is the risk of criminals counterfeiting electronic money, which is heightened if banks fail to incorporate adequate measures to detect and deter counterfeiting. A bank faces operational risk from counterfeiting, as it may be liable for the amount of the falsified electronic money balance. In addition, there may be costs associated with repairing a compromised system.

2.1.2 Systems design, implementation, and maintenance

A bank faces the risk that the systems it chooses are not well designed or implemented. For example, a bank is exposed to the risk of an interruption or slow-down of its existing systems if the electronic banking or electronic money system it chooses is not compatible with user requirements.

Many banks are likely to rely on outside service providers and external experts to implement, operate, and support portions of their electronic money and electronic banking activities. Such reliance may be desirable because it allows a bank to outsource aspects of the provision of electronic banking and electronic money activities that it cannot provide economically itself. However, reliance on outsourcing exposes a bank to operational risks. Service providers may not have the requisite expertise to deliver services expected by the bank, or may fail to update their technology in a timely manner. A service provider's operations could be interrupted due to system breakdowns or financial difficulties, jeopardising a bank's ability to deliver products or services.

The rapid pace of change that characterises information technology presents banks with the risk of systems obsolescence. For example, computer software that facilitates the use of electronic banking and electronic money products by customers will require updating, but channels for distributing software updates pose risks for banks in that criminal or malicious individuals could intercept and modify the software. In addition, rapid technological change can mean that staff may fail to understand fully the nature of new technology employed by the bank. This could result in operational problems with new or updated systems.

2.1.3 Customer misuse of products and services

As with traditional banking services, customer misuse, both intentional and inadvertent, is another source of operational risk. Risk may be heightened where a bank does not adequately educate its customers about security precautions. In addition, in the absence of adequate measures to verify transactions, customers may be able to repudiate transactions they previously authorised, inflicting financial losses on the bank. Customers using personal information (e.g., authentication information, credit card numbers or bank account numbers) in a non-secure electronic transmission could allow criminals to gain access to customer

accounts. Subsequently, the bank may incur financial losses because of transactions customers did not authorise. Money laundering may be another source of concern, as pointed out in the Group of Ten, April 1997, report: *Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross-Border Issues.*

2.2. Reputational risk

Reputational risk is the risk of significant negative public opinion that results in a critical loss of funding or customers. Reputational risk may involve actions that create a lasting negative public image of overall bank operations, such that the bank's ability to establish and maintain customer relationships is significantly impaired. Reputational risk may also arise if actions by the bank cause a major loss of public confidence in the bank's ability to perform functions critical to its continued operation. Reputational risk can arise in response to actions a bank itself takes, or in response to actions of third parties. Increased reputational risk can be a direct corollary of heightened risk exposure, or problems, in other risk categories, particularly operational risk.

Reputational risk may arise when systems or products do not work as expected and cause widespread negative public reaction. A significant breach of security, whether as a result of external or internal attacks on a bank's system, can undermine public confidence in a bank. Reputational risk may also arise in cases where customers experience problems with a service but have not been given adequate information about product use and problem resolution procedures.

Mistakes, malfeasance, and fraud by third parties may also expose a bank to reputational risk. Reputational risk can arise from significant problems with communications networks that impair customers' access to their funds or account information, particularly if there are no alternative means of account access. Substantial losses caused by mistakes of another institution offering the same, or similar, electronic banking or electronic money products or service may cause a bank's customers to view its products or service with suspicion, even if the bank itself did not face the same problems. Reputational risk may also arise from targeted attacks on a bank. For example, a hacker penetrating a bank's web site may alter it to intentionally spread inaccurate information about the bank or its products.

Reputational risk may not only be significant for a single bank but also for the banking system as a whole. If, for instance, a globally active bank experienced important reputational damage concerning its electronic banking or electronic money business, the security of other banks' systems may also be called into question. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system as a whole.

2.3. Legal risk

Legal risk arises from violations of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. Given the relatively new nature of many retail electronic banking and electronic money activities, rights and obligations of parties to such transactions are, in some cases, uncertain. For example, application of some consumer protection rules to electronic banking and electronic money activities in some countries may not be clear. In addition, legal risk may arise from uncertainty about the validity of some agreements formed via electronic media.

Electronic money schemes may be attractive to money launderers if the systems offer liberal balance and transaction limits, and provide for limited auditability of transactions. Application of money laundering rules may be inappropriate for some forms of electronic payments. Because electronic banking can be conducted remotely, banks may face increased difficulties in applying traditional methods to prevent and detect criminal activity.

Banks engaging in electronic banking and electronic money activities can face legal risks with respect to customer disclosures and privacy protection. Customers who have not been adequately informed about their rights and obligations may bring suit against a bank. Failure to provide adequate privacy protection may also subject a bank to regulatory sanctions in some countries.

Banks choosing to enhance customer service by linking their Internet sites to other sites also can face legal risks. A hacker may use the linked site to defraud a bank customer, and the bank could face litigation from the customer.

As electronic commerce expands, banks may seek to play a role in electronic authentication systems, such as those using digital certificates.[7] The role of a certification authority may expose a bank to legal risk. For example, a bank acting as a certification authority may be liable for financial losses incurred by parties relying on the certificate. In addition, legal risk could arise if banks participate in new authentication systems and rights and obligations are not clearly specified in contractual agreements.

---

[7] A digital certificate issued by a certification authority is intended to ensure that a given digital signature is in fact generated by a given signer. A bank that undertakes to act as a certification authority could be considered to be providing services to clients similar to those associated with providing an account access device or acting as a notary public. A digital signature is a string of data appended to an electronic message that is intended to identify uniquely the sender to the recipient. At present, most digital signatures are generated using a cryptographic algorithm in which the sender uses one mathematical function to create the signature and the receiver uses a different, but related mathematical function to verify the signature. Digital signatures also typically provide a mechanism for verifying the integrity of the message.

2.4. Other risks

Traditional banking risks such as credit risk, liquidity risk, interest rate risk, and market risk may also arise from electronic banking and electronic money activities, though their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational, and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialise in electronic banking and electronic money activities.

2.4.1 Credit risk is the risk that a counterparty will not settle an obligation for full value, either when due or at any time thereafter. Banks engaging in electronic banking activities may extend credit via non-traditional channels, and expand their market beyond traditional geographic boundaries. Inadequate procedures to determine the creditworthiness of borrowers applying for credit via remote banking procedures could heighten credit risk for banks. Banks engaged in electronic bill payment programs may face credit risk if a third party intermediary fails to carry out its obligations with respect to payment. Banks that purchase electronic money from an issuer in order to resell it to customers are also exposed to credit risk in the event the issuer defaults on its obligations to redeem the electronic money.

2.4.2 Liquidity risk is the risk arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses, although the bank may ultimately be able to meet its obligations. Liquidity risk may be significant for banks that specialise in electronic money activities if they are unable to ensure that funds are adequate to cover redemption and settlement demands at any particular time. In addition, failure to meet redemption demands in a timely manner could result in legal action against the institution, and lead to reputational damage.

2.4.3 Interest rate risk refers to the exposure of a bank's financial condition to adverse movements in interest rates. Banks specialising in the provision of electronic money may face significant interest rate risk to the extent adverse movements in interest rates decrease the value of assets relative to electronic money liabilities outstanding.

2.4.4 Market risk is the risk of losses in on- and off-balance sheet positions arising from movements in market prices, including foreign exchange rates. Banks accepting foreign currencies in payment for electronic money are subject to this type of risk.

2.5. Cross border issues

Electronic banking and electronic money activities are based on technology that by its very nature is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders, highlighting certain risks. Although banks currently face similar types of risks in international banking, it is important to note that these risks are also relevant to the cross-border conduct of electronic banking and electronic

money. Banks may face different legal and regulatory requirements when they deal with customers across national borders. For new forms of retail electronic banking, such as Internet banking, and for electronic money, there may be uncertainties about legal requirements in some countries. In addition, there may be jurisdictional ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risk associated with non-compliance with different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules, and money laundering laws.

Operational risk could arise for a bank dealing with a service provider located in another country, which for that reason may be more difficult to monitor. Banks may also face other risks as they engage in the provision of electronic banking and electronic money activities across borders. Banks dealing with foreign-based service providers, or with foreign participants in electronic banking or electronic money activities, are subject to country risk to the extent that foreign parties become unable to fulfil their obligations due to economic, social, or political factors. A bank offering services via open networks like the Internet may be exposed to credit risk, in that applications for credit from customers in other countries may be more difficult to evaluate with procedures based upon a more familiar customer base. Banks accepting foreign currencies in payment for electronic money may be subject to market risk because of movements in foreign exchange rates.

3. Risk management

For an increasing number of banks there may be a strategic reason for engaging in electronic banking and electronic money activities. In addition, greater use of electronic banking and electronic money may increase the efficiency of the banking and payment system, benefiting consumers and merchants. At the same time, as the preceding discussion indicates, there are risks for banks engaging in electronic banking and electronic money activities. Risks must be balanced against benefits; banks must be able to manage and control risks and absorb any related losses if necessary. Risks from electronic banking and electronic money activities should also be evaluated in the context of other risks the bank faces. Even though electronic banking and electronic money activities may represent a relatively small portion of the overall activities of banks currently, supervisors may still require senior management's assurance that critical systems are not threatened by the risk exposures banks take.

The rapid pace of technological innovation is likely to change the nature and scope of risks banks face in electronic money and electronic banking. Supervisors expect banks to have processes that enable bank management to respond to current risks, and to adjust to new risks. A risk management process that includes the three basic elements of *assessing* risks, *controlling* risk exposure, and *monitoring* risks will help banks and supervisors attain these goals. Banks may employ such a process when committing to new

electronic banking and electronic money activities, and as they evaluate existing commitments to these activities.

It is essential that banks have a comprehensive risk management process in place that is subject to appropriate oversight by the board of directors and senior management. As new risks in electronic banking and electronic money activities are identified and assessed, the board and senior management must be kept informed of these changes. Prior to any new activity being commenced, a comprehensive review should be conducted so that senior management can ensure that the risk management process is adequate to assess, control and monitor any risks arising from the proposed new activity.

3.1. Assessing risks

Assessing risks is an ongoing process. It typically involves three steps. First, a bank may engage in a rigorous analytic process to identify risks and, where possible, to quantify them. In the event risks cannot be quantified, management may still identify how potential risks can arise and the steps it has taken to deal with and limit those risks. Bank management should form a reasonable and defensible judgement of the magnitude of any risk with respect to both the impact it could have on the bank (including the maximum potential impact), and the probability that such an event will occur.

A second step in assessing risk is for the board of directors or senior management to determine the bank's risk tolerance, based on an assessment of the losses the bank can afford to sustain in the event a given problem materialises. Finally, management can compare its risk tolerance with its assessment of the magnitude of a risk to ascertain if the risk exposure fits within the tolerance limits.

3.2. Managing and controlling risks

Having made an assessment of risks and its risk tolerance, bank management should take steps to manage and control risks. This phase of a risk management process includes activities such as implementing security policies and measures, co-ordinating internal communication, evaluating and upgrading products and services, implementing measures to ensure that outsourcing risks are controlled and managed, providing disclosures and customer education, and developing contingency plans. Senior management should ensure that staff responsible for enforcing risk limits have authority independent from the business unit undertaking the electronic banking or electronic money activity. Banks increase their ability to control and manage the various risks inherent in any activity when policies and procedures are set out in written documentation and made available to all relevant staff.

3.2.1 Security policies and measures

Security is the combination of systems, applications, and internal controls used to safeguard the integrity, authenticity, and confidentiality of data and operating processes. Proper security relies on the development and implementation of adequate security policies and security measures for processes within the bank, and for communication between the bank and external parties. Security policies and measures can limit the risk of external and internal attacks on electronic banking and electronic money systems, as well as the reputational risk arising from security breaches.

A *security policy* states management's intentions to support information security and provides an explanation of the bank's security organisation. It also establishes guidelines that define the bank's security risk tolerance. The policy may define responsibilities for designing, implementing, and enforcing information security measures, and it may establish procedures to evaluate policy compliance, enforce disciplinary measures, and report security violations.

Security measures are combinations of hardware and software tools, and personnel management, that contribute to building secure systems and operations. Senior management should regard security as a comprehensive process that is only as strong as the weakest link in the process. Banks can choose from a variety of security measures to prevent or mitigate external and internal attacks and misuse of electronic banking and electronic money. Such measures include, for example, encryption, passwords, firewalls, virus controls, and employee screening. Encryption is the use of cryptographic algorithms to encode clear text data into cipher text to prevent unauthorised observation.[8] Passwords, pass phrases, personal identification numbers, hardware-based tokens, and biometrics are techniques for controlling access and identifying users.

Firewalls are combinations of hardware and software that screen and limit external access to internal systems connected to open networks such as the Internet. Firewalls may also separate segments of internal networks using Internet technology (Intranets). Firewall technology, if properly designed and implemented, can be an effective means of controlling access and safeguarding data confidentiality and integrity. Because this technology is complex to design and can be costly, its strength and capabilities should be proportionate with the sensitivity of the information being protected. A well-planned design should include enterprise-wide security requirements, clear procedures for operation, separation of duties, and selection of trusted personnel who are responsible for the configuration and operation of the firewall.

---

8 See *Security of Electronic Money*, Bank for International Settlements, August 1996, especially section 4.1.2 on cryptography, for a detailed discussion of encryption.

Although firewalls screen incoming messages they do not necessarily protect against virus-infected programs downloaded from the Internet. As a consequence, management should develop prevention and detection controls to reduce the chance of virus attack and data destruction, particularly for remote banking. Programmes to mitigate the risk of a virus infection may include network controls, end-user policies, user training, and virus detection software.

Not all security threats are external. Electronic banking and electronic money systems should also be safeguarded, to the extent possible, against unauthorised activities by current and former employees. As with existing banking activities, background checks for new employees, temporary employees, and consultants, as well as internal controls and separation of duties are important precautions to protect system security.

For electronic money, additional security measures may help deter attacks and misuse, including counterfeiting and money laundering.[9] Such measures could include on-line interaction with the issuer or a central operator; monitoring and tracing individual transactions; maintenance of cumulative records in a central database; the use of tamper-resistant devices incorporated into stored-value cards and merchant hardware; and the use of value limits and expiration dates on stored-value cards.

3.2.2 Internal communication

Aspects of operational, reputational, legal, and other risks can be managed and controlled if senior management communicates to key staff how the provision of electronic banking and electronic money is intended to support the overall goals of the bank. At the same time, technical staff should clearly communicate to senior management how systems are designed to work, as well as the strengths and weaknesses of systems. Such procedures can reduce operational risks of poor systems design, including incompatibility of different systems within a banking organisation; data integrity problems; reputational risk associated with customer dissatisfaction that systems did not work as expected; and credit and liquidity risk.

To ensure adequate internal communication, all policies and procedures should be provided in writing. In addition, senior management should adopt a corporate policy of ongoing education and upgrading of skills and knowledge, consistent with the pace of technological innovation, in order to limit operational risks arising from lack of staff and management expertise. Training may include technical course work, as well as time for staff to keep abreast of important market developments.

---

9 A detailed discussion of security measures for electronic money can be found in *Security of Electronic Money*, Bank for International Settlements, April 1996. That report concluded that a combination of security measures, rather than reliance on any one particular measure, is likely to be most effective in preventing and deterring security problems for electronic money.

3.2.3 Evaluating and upgrading

Evaluating products and services before they are introduced on a widespread basis can also help limit operational and reputational risks. Testing validates that equipment and systems function properly and produce the desired results. Pilot programs or prototypes can be helpful in developing new applications. The risk of system slowdowns or disruptions can also be reduced by policies to review the capabilities of existing hardware and software regularly.

3.2.4 Outsourcing

A growing trend in the industry is for banks to focus strategically on core competencies and rely on external parties specialising in activities outside the bank's expertise. While these arrangements may offer benefits such as cost-reduction and economies of scale, outsourcing does not relieve the bank of the ultimate responsibility for controlling risks that affect its operations. Consequently, banks should adopt policies to limit risks arising from reliance on outside service providers. For example, bank management should monitor the operational and financial performance of their service providers; ensure that contractual relations between parties, as well as the expectations and obligations of each party, are clearly understood and are defined in written, enforceable contracts; and maintain a contingency arrangement to change service providers in a prompt manner, if necessary.

Security of the bank's sensitive information is of critical importance. The outsourcing arrangement may require the bank to share sensitive data with service providers. Bank management should evaluate the ability of the service provider to maintain the same level of security as though the activities were conducted in-house, through the review of service providers' policies and procedures aimed at protecting sensitive data. Additionally, supervisors may wish to have the right to independently assess, when necessary, the competence and the operational and financial performance of the service providers.

3.2.5 Disclosures and customer education

Disclosures and customer education may help a bank limit legal and reputational risk. Disclosures and programs to educate customers that address how to use new products and services, fees charged for services and products, and problem and error resolution procedures can help banks comply with customer protection and privacy laws and regulations. Disclosures and explanations about the nature of a bank's relationship to a linked web site may help reduce legal risk to a bank arising from problems with services or products on the linked sites.

3.2.6 Contingency planning

A bank can limit the risk of disruptions in internal processes or in service or product delivery by developing contingency plans that establish its course of action in the

event of a disruption in its provision of electronic banking and electronic money services. The plan may address data recovery, alternative data-processing capabilities, emergency staffing, and customer service support. Backup systems should be tested periodically to ensure their continuing effectiveness. Banks should ensure that their contingency operations are as secure as their normal production operations.

An important aspect of electronic banking and electronic money is the reliance on external entities including hardware vendors, software providers, Internet service providers, and telecommunications companies. Bank management may insist that such service providers have backup capabilities. In addition, management may consider compensating actions it can take in the event service providers become impaired. Such plans could include short-term contracting with other providers, and a policy describing how the bank will address customer losses associated with the service disruption. Banks should also consider the advisability of reserving the right to change service providers in a prompt manner if necessary.

Contingency planning may also contribute to limit reputational risk arising from the bank's own actions, or from problems experienced by another institution offering the same or similar electronic banking or electronic money products or services. For example, banks may wish to establish procedures to address customer problems during system disruptions.

3.3. Monitoring risks

Ongoing monitoring is an important aspect of any risk management process. For electronic banking and electronic money activities, monitoring is particularly important both because the nature of the activities are likely to change rapidly as innovations occur, and because of the reliance of some products on the use of open networks such as the Internet. Two important elements of monitoring are system testing and auditing.

3.3.1 System testing and surveillance

Testing of systems operations can help detect unusual activity patterns and avert major system problems, disruptions, and attacks. Penetration testing focuses upon the identification, isolation, and confirmation of flaws in the design and implementation of security mechanisms through controlled attempts to penetrate a system outside normal procedures. Surveillance is a form of monitoring in which software and audit applications are used to track activity. In contrast to penetration testing, surveillance focuses on monitoring routine operations, investigating anomalies, and making ongoing judgements regarding the effectiveness of security by testing adherence to security policies.

3.3.2 Auditing

Auditing (internal and external) provides an important independent control mechanism for detecting deficiencies and minimising risks in the provision of electronic

banking and electronic money services. The role of an auditor is to ensure that appropriate standards, policies, and procedures are developed, and that the bank consistently adheres to them. Audit personnel must have sufficient specialised expertise to perform an accurate review. An internal auditor should be separate and independent from employees making risk management decisions. To augment internal audit, management may seek qualified external auditors, such as computer security consultants or other professionals with relevant expertise, to provide an independent assessment of the electronic banking or electronic money activity.

3.4. Management of cross border risks

Cross border risks may be more complex than risks banks face within their home country. Hence, banks and supervisors may need to devote added attention to assessing, controlling, and monitoring operational, reputational, legal and other risks arising from cross border electronic banking and electronic money activities.

Banks that choose to provide services to customers in different national markets will need to understand different national legal requirements, and develop an appreciation for national differences in customer expectations and knowledge of products and services. In addition, senior management should ensure that existing systems for credit extension and liquidity management take into account potential difficulties arising from cross border activities. A bank may need to assess country risk and develop contingency plans that take into account service disruptions due to problems in the economic or political climate abroad. A bank may also face difficulties in enforcing the fulfilment of a foreign service provider's obligations. In the case of banks relying on service providers located abroad, national supervisors may want to assess the accessibility of information from, and consider the activities of, cross-border service providers on a case-by-case basis.

National supervisors can play an important role by identifying and discussing jurisdictional ambiguities. They can also continue efforts to develop measures to detect unsafe and illegal practices. Finally, national supervisors can continue, and strengthen, cooperative efforts to share information about product and service innovations and industry practices.

ANNEX

Examples of possible risks and risk management measures in retail electronic banking and electronic money

The matrix below provides examples of possible risks banks may face in engaging in electronic banking and electronic money activities, and notes possible measures banks may use to manage such risks. The list is representative rather than exhaustive. The possible risk management measures should not be construed as a reflection of national or international supervisory policy.

Examples of possible risks and risk management measures in retail electronic banking and electronic money

Examples of possible risks	Possible manifestation	Potential effect on the banking organisation	Possible risk management measures
Operational risk			
Unauthorized system access.	Hacker gains entry to internal systems. Confidential customer information is intercepted by an unauthorized third party. Virus injected into bank's system. Bank's systems and data deliberately corrupted and crashed.	Loss of data. Theft of, or tampering with, customer information. Disabling of a significant portion of bank's internal computer system. Costs associated with repairing system. Perceived insecurity of bank's systems and potential adverse publicity.	Penetration testing for vulnerabilities. Surveillance to detect anomalies in usage. Deployment of communication security measures such as firewalls, password management, encryption techniques, and proper authorization of end-users. Deploy virus checking and on-going monitoring of security measures in internal systems.
Employee fraud.	Employee alteration of data in order to draw funds from general bank accounts, and to obtain information from records. Employee theft of smart cards.	Costs associated with reimbursing customer losses and with reconstructing accurate data on customers. Possible losses from redeeming electronic money for which no corresponding prepaid funds were received. Customers may perceive the bank as being unreliable. A bank may face legal or regulatory sanctions, and negative publicity.	Develop policies for adequately screening new employees. Institute internal controls, including segregation of duties. External auditing of employee performance. Proper control over storage, manufacture, etc. of smart cards.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Counterfeiting of electronic money.	Criminals alter or duplicate electronic money products to obtain goods or funds without proper payment.	A bank may be liable for the amount of the falsified electronic money. Possible costs associated with repairing a compromised system.	On-line interaction with the issuer or central operator; monitor and trace individual transactions; maintain cumulative records in a central database; incorporate tamper-resistant devices into stored-value cards and merchant hardware; develop audit trails. Low load-limits may make counterfeiting less attractive for criminals.
Service provider risk.	Service provider may not deliver services expected by the bank; deficiencies in system or data integrity or reliability may result.	Bank may be held accountable by customers for service provider-induced problems.	Undertake due diligence before entering into a service provider contract. Construct service provider contracts that establish performance benchmarks, and address contingencies and auditing provisions. Establish backup plans with service provider; develop contingency plans for contracting with alternative service providers.
Obsolescence of systems.	Delays or disruptions in processing transactions. Deficiencies in system or data integrity or reliability.	Adverse public reaction. Possible legal repercussions as law suits could result from erroneous transactions. Costs associated with resolving customer problems.	Regular review of capabilities of existing hardware and software. Installation of an accountability system that assigns responsibility for updates to systems and equipment.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Outdated staff and management expertise.	Rapid technological change can mean that management and staff at a bank are not able to fully understand the nature of new technology employed by the bank, or technological upgrades provided by service providers.	Poor implementation of newer technology. Inability to provide ongoing support. Deficiencies in system or data integrity or reliability.	Develop corporate view of training as an ongoing process. Design management and staff training at the planning stage.
Inadequate customer security practices.	Customer use of personal information (e.g., credit card numbers, bank account numbers) in non-secure electronic transmissions. Criminals could access customer accounts using what should be kept as confidential information.	Financial loss through unauthorized transactions.	Provide information to customers on the importance of safeguarding information in non-secure transactions. Incorporate security measures into products and services.
Customer repudiation of a transaction.	Customer completes a transaction, but denies transaction took place, and demands reimbursement of funds.	Expenses incurred in proving that the customer authorized the transaction. Possible loss of funds if proof cannot be produced.	Implement security measures that enhance customer authentication, such as personal identification numbers. Audit trail for transactions.
Reputational risk			
Significant, widespread system deficiencies.	Customers' access to their funds or account information is impaired.	Customers may discontinue use of the product or the service. Directly affected customers leave the bank; others follow if problems are publicized.	Test systems before implementing. Develop back-up facilities and contingency plans, including plans to address customer problems during system disruptions.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
A significant breach of security.	A virus is introduced into a bank's system, causing significant system and data integrity problems. Hackers gain entry to internal systems.	Customers may discontinue use of the product or the service. Directly affected customers leave the bank; others follow.	Penetration testing, and other appropriate security measures. Develop contingency plans. Deploy virus checking.
Problems with, or misuses of, same or similar systems or products by another institution.	Customers view a given bank's electronic money with suspicion in the wake of problems by another bank.	Customers may leave the bank.	Develop contingency plans.
Legal risk			
Uncertain or ambiguous applicability of laws and rules.	A bank may inadvertently be in noncompliance with laws. Application of established consumer compliance rules, money-laundering rules, and signature rules may be uncertain.	A bank may incur legal expenses, or be subject to regulatory sanctions.	Ascertain areas of legal uncertainty prior to committing to electronic money or electronic banking activities. Make careful judgments about risk tolerance for legal uncertainties. Perform periodic compliance reviews. Request interpretations from regulatory authorities. Update compliance training. Develop contingency plans.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Money laundering.	A bank's electronic banking or electronic money system may be misused by customers who seek to engage in criminal activity, including money laundering.	Legal sanctions for noncompliance with "know your customer" laws.	Design customer identification and screening techniques. Develop audit trails. Design policies and procedures to spot and report suspicious activities. For electronic money, low load limits may make money laundering less attractive. Perform periodic compliance reviews. Update compliance training. Develop contingency plans.
Inadequate disclosure of information to customers.	Customers may not fully understand what their rights and obligations are, including, for example, any dispute resolution procedure. They may therefore take inadequate precautions in using the product or service.	Customer may bring legal suit against the bank as a result of losses or disputed transactions. A bank may be subject to regulatory or legal sanctions.	Ascertain appropriate disclosures in advance of offering electronic money or electronic banking activities. Train employees to be aware of typical difficulties customers may have. Carefully weigh costs and benefits of disclosures beyond legal minimum in areas where customer risks may arise. Design and disseminate product information to the public. Develop a process to periodically review regulatory requirements.
Failure to protect customer privacy.	A bank releases information profiling the pattern of customer financial transactions without customer authorization.	Litigation expenses incurred by bank if law suits are filed by customers. Bank may face legal or regulatory sanctions.	Review privacy protection policies. Train employees in privacy protection procedures. Deploy security measures. Perform periodic compliance reviews. Update compliance training.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Problems at a linked Internet site.	A bank may link its web site to web sites of entities offering complementary products. The linked site may disappoint or defraud a bank customer.	The bank could face litigation from the customer.	Fully understand the legal repercussion, and security risks, of linking to other web sites. Make appropriate consumer disclosures to prevent consumer confusion over the role of the bank, or the insured status of products offered at linked sites. Do not make representations on bank's site regarding the quality of the goods or services available at the linked sites.
Certificate authority risk.	Forged certificates are issued in the bank's name, defrauding customers. Certificates are issued to persons posing as bank customers without adequate identity verification.	Costs associated with revoking and reissuing compromised certificates. Parties relying on a forged or fraudulently obtained certificate may bring lawsuits against the bank. Negative reputational repercussions.	Implement appropriate security measures and controls.
Exposure to foreign jurisdictions.	A bank offering services over the Internet may attract customers from other countries, causing the bank to be subject to different legal or regulatory requirements. Ambiguities about jurisdictional responsibilities of different national authorities. Bank-issued or distributed electronic money may be used outside the country in which the bank is chartered.	A bank may be in noncompliance with laws or regulations outside its home country. A bank may incur unanticipated legal expenses.	Ascertain the extent to which its electronic money and electronic banking activities are likely to be used across borders, and make careful judgments on the bank's ability to respond to legal and jurisdictional uncertainties. Train personnel about different national legal and regulatory environments.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Credit risk			
Default of borrowers who applied for credit via remote banking.	Bank may approve extension of credit to customers outside its normal market where data are not available, or are costly to obtain.	Unanticipated provisioning for non-performing loans may be necessary.	Ensure that evaluation of creditworthiness of remote banking customers is in line with traditional requirements. Audit lending decisions and procedures.
Default of an electronic money issuer.	Issuer may become insolvent while the bank holds electronic money for resale to customers or for redemption.	A bank may have to use its own funds to redeem electronic money held by its customers in the event of issuer default.	Perform due diligence on any issuing entity prior to participating in an electronic money system. Monitor the financial condition of the issuer. Develop contingency plans in case of default.
Liquidity risk			
Illiquidity of electronic money issuer.	A sudden increase in demand for redemption of electronic money. May be a problem for banks that specialise in electronic money schemes.	Bank may incur losses as it seeks to generate more costly sources of funds. If public perceives liquidity problems there may be a more widespread withdrawal of deposits or redemption of electronic money. Failure to meet redemption demands in a timely manner could also lead to reputation damage.	Invest funds in liquid assets. Develop a monitoring system on usage. Conduct regular and comprehensive audits.

Examples of possible risks	**Possible manifestation**	**Potential effect on the banking organisation**	**Possible risk management measures**
Interest rate risk			
Unanticipated interest rate changes for instruments in which an electronic money issuer invests.	Unfavorable movement in interest rates could decrease value of assets relative to electronic money liabilities outstanding. May be a problem for banks that specialise in electronic money issuance.	Unanticipated decline in value of assets could bring bank out of compliance with regulatory requirements. Liquidity problems could arise.	Institute interest rate risk management measures commensurate with bank's exposure.
Market risk			
Foreign Exchange risk arising from acceptance of foreign currencies in payment for electronic money.	An unfavorable movement in FX rates could require bank to cover losses.	Negative impact on earnings.	Establish FX risk management or hedging program.
Country risk			
Transfer risk arising from foreign-based service provider, foreign participants in an electronic money or electronic banking scheme.	Foreign service providers or participants in an electronic money or electronic banking scheme may become unable to fulfill obligations due to economic, social, or political factors.	Costs of resolving customer problems. The bank could face litigation from the customer.	Conduct country risk assessment. Develop contingency plans for contracting with other possible participants.