GUIDELINES FOR ELECTRONIC BANKING

NOVEMBER 2002

TABLE OF CONTENTS

GUIDELINES FOR ELECTRONIC BANKING

1. FOREWORD

This document is intended to provide guidance on the promotion of safe and sound e-banking[1] activities, while preserving the flexibility necessary to accommodate future technological and other changes. The guidelines are general since the Central Bank of Barbados is of the view that setting too detailed requirements in the area of e-banking could lead to their becoming rapidly outdated. The document is not intended to create new examination standards, impose regulatory requirements or represent an exclusive description of the various ways that banks can implement effective information security programs. Whether financial institutions contract with third-party providers[2] for e-banking services (such as Internet banking) or maintain computer services in-house, bank management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks.

We advocate that if a bank is relying on third-party providers in this regard, management must generally understand the provider's information security program to effectively evaluate the security system's ability to protect bank and customer data. Furthermore, while these guidelines are representative of current sound industry practice, they should not be considered unchangeable, since many security controls and other risk management techniques will continue to evolve rapidly in order to keep pace with new technologies and business applications.

1 Refers to banking activity being facilitated electronically, i.e. through a computer or some other intelligent device.

2 For the purposes of this guidance, "third-party provider" is broadly defined as suppliers that may provide the following services or products to institutions: system design, development, administration, and maintenance services, data processing services; and system solutions.

SECTION 1

1. INTRODUCTION AND BACKGROUND

In many ways, e-banking is not unlike traditional payment, inquiry, and information processing systems, differing only in that it utilises a different delivery channel. Any decision to adopt e-banking is normally influenced by a number of factors. These include customer service enhancement and competitive costs, all of which motivate banks to assess their electronic commerce strategies. The benefits of e-banking are widely known and will only be summarised briefly in this document.

E-banking can improve a bank's efficiency and competitiveness, so that existing and potential customers can benefit from a greater degree of convenience in effecting transactions. This increased level of convenience offered by the bank, when combined with new services, can expand the bank's target customers beyond those in traditional markets. Consequently, financial institutions are therefore becoming more aggressive in adopting electronic banking capabilities that include sophisticated marketing systems, remote-banking capabilities, and stored value programs. Internationally, familiar examples include telephone banking, automated teller networks, and automated clearinghouse systems. Such technological advances have brought greater sophistication to all users, commercial and "the man in the street".

A bank may be faced with different levels of risks and expectations arising from electronic banking as opposed to traditional banking. Furthermore, customers who rely on e-banking services may have greater intolerance for a system that is unreliable or one that does not provide accurate and current information. Clearly, the longevity of e-banking depends on its accuracy, reliability and accountability. The challenge for many banks is to ensure that savings from the electronic banking technology more than offset the costs and risks involved in such changes to their systems.

2. BRIEF OVERVIEW OF THE CURRENT STATE OF E-BANKING IN BARBADOS

By the end of the 1990's electronic banking in Barbados had risen sharply with many bank consumers using automated teller machines (ATM) and other electronic facilities on offer by local commercial banks. Though much of the use of the ATM occurred in many instances through cost saving measures[3] on the part of the consumer, many have recognised the benefits in terms of time saving and convenience. Therefore, the ATM has become the most popular form of electronic banking in Barbados, and all banks, and even some credit unions, now have ATM facilities. This is not, however, the only form of e-banking in Barbados, since some banks also offer telephone/voice recognition banking, the use of debit cards, point-of-sale (POS) purchases and electronic funds transfer. These services on offer represent the basic form of e-banking. However, offering the next level of e-banking, such as Internet or personal computer (PC) banking requires a certain set of prerequisites before it can be offered efficiently and safely.

Of the seven commercial banks in Barbados, only one possesses a website, which can be categorised as a Level I system according to the categories in the last chapter. This bank provides only basic – mainly promotional - information on its website. Even though some of these banks are branches and subsidiaries of larger international operations, they have not transposed head-office systems to Barbadian operations. To some, in this context, it may be considered as regressive, but there are clear reasons for this, mainly costs, risks, and demand. Implementing a fully functional and efficient PC banking system is costly. Even though in the long-run banks will save per transaction, they still need sufficient volume to amortise this cost over time, and for the most part this volume does not yet exist. Another cause for this slow response is risk. Many of these systems expose banks to large-scale risks that can jeopardise Barbadian banks' small capital base.

3 During the late 1990's most banks began instituting bank charges for teller services over a specified number of transactions, largely in an effort to entice consumers to increase their use of the ATMs, which are cheaper per transaction compared to teller service, and in many instances were underutilised.

For with Internet banking the systems of commercial banks in Barbados are now exposed globally. Essentially, on a risk-adjusted scale, banks do not seem to have been convinced of the feasibility of a wide-scale offer of PC-banking services. There is also a lack of demand because Barbados is - to a large extent - a cash-based society and banking cards are not very widely used. Therefore, the demand for PC-banking services is not evident even though the level of Internet penetration is increasing. A further education by both the public and private sector on the benefits of using some of these more 'sophisticated' banking services may be warranted before there can be a surge in the use of electronic banking, or before there is general acceptance of electronic banking.

Most commercial entities in Barbados have not effectively acknowledged the need for e-commerce, and in some cases may have determined that it is not cost effective to offer such services. This lack of enthusiasm among the private sector has led to knock-on effects. For offering back-up services to these entities, commercial banks may incur some costs in providing some cover for risks emanating from operating in this electronic environment, such as charge-back costs. Those companies that pose the greatest threat to commercial banks are high volume and high-risk websites.

However, following a thrust from the public sector and some areas of the private sector into e-commerce and a promotion of the benefits that it can provide, some banks have been actively seeking to build their capabilities and capacity to offer such services. A number of them have highlighted system readiness for other levels of retail e-banking within another two or three years. Much of the development of these systems is being implemented internally, but with assistance from external elements and from head offices or affiliates. Most have indicated that they possess the institutional capacity to offer such services without any large increase in risk to the financial system. However, they are untested and before they could reach the roll-out stage there will be an extended period of stress testing, especially to conform to Central Bank of Barbados' safety concerns.

1.1 Electronic Capabilities

Electronic capabilities can be segregated into three (3) categories by degree of functionality. These levels range from Level I to Level III systems.

Level 1 - Information-Only Systems

Banks should ensure that consumers are alerted to the potential risks associated with unencrypted electronic mail sent over such a medium. Information-only systems are defined as those that allow access to general-purpose marketing and other publicly available information, or the transmission of non-sensitive electronic mail.

Level 2 - Electronic Information Transfer Systems

Since communication and system security risks include data privacy and confidentiality, data integrity, authentication, non-repudiation, and access system design, some risk mitigation methods are therefore necessary. Electronic information transfer systems are interactive in that they provide the ability to transmit sensitive messages, documents, or files among a group of users, for example, a bank's web site that allows a customer to submit online loan or deposit account applications.

Level 3 - Fully Transactional Information Transfer Systems

Fully Transactional Information Transfer Systems represent the highest degree of functionality and also involve high levels of potential risks. These systems provide the capabilities for information-only applications, electronic information transfer systems, as well as online, transactional banking services. These capabilities are provided by interactive connectivity between a customer's device and the bank's internal systems. Many systems will however involve a combination of these capabilities.

1.2 The Networked Environment

Each bank must evaluate the risk it faces and its readiness to react to those risks. Electronic banking relies on a networked environment, such as the Internet. Importantly, not all networks carry the same degree of risk, and so not all networks are equally

vulnerable or sensitive. Although the current dollar volume of e-banking activity is small relative to the overall financial activity, the associated risks can be significant. Electronic banking can substantially increase access to a bank's internal systems via public networks, and expose those systems to hackers, viruses and other forms of risk.

Any reliance on service providers and software vendors for e-banking will require sound risk management practices. Typically, e-banking can increase a bank's reliance on service providers and software vendors who design, implement, or even manage these electronic systems. The degree to which banks choose to operate their systems through service providers and software vendors will affect the extent of the bank's involvement in actual systems design, planning, and other day-to-day operational and monitoring issues. Essentially, banks that outsource all of these functions will initially have less "hands on" involvement in detecting unauthorized intrusions into a bank's e-banking system, compared with banks that perform some or all of their security and operational functions in-house.

Risk identification and analysis should direct the bank to adopt appropriate oversight and review guidelines, operating policies and procedures, audit requirements, and contingency plans. These risks can be mitigated by adopting a comprehensive risk management programme that incorporates a sound strategic plan. Importantly, the extent of a financial institution's risk management programme should be commensurate with the complexity and sophistication of the activities in which it engages. Essentially, a bank which offers a simple information-only site is generally not expected to have undertaken the same level of planning and risk management as institutions that engage in more complex activities.

SECTION 2

2. ELECTRONIC BANKING RISKS AND CONTROLS

2.1 Overview

Each financial institution should apply guidelines based on its scope and level of sophistication. Typically, electronic banking amplifies the scale of exposure of banks to traditional risks, such as transaction, strategic, reputational, and compliance risk, among others. Many of these risk categories have been identified in the Basel Committee's *Core Principles for Effective Banking Supervision*, published in September 1997.

As information systems become more connected and interdependent, the risk of computer intrusion will increase. Arguably, this is the single most important aspect of the 'new' electronic delivery system. Banks with weak physical security and systems substantially increase their exposure to a plethora of risks, many of which could lead to collapse. Potential consequences include direct dollar loss, damaged reputation, improper disclosure, and lawsuits or regulatory sanction.

E-banking should be consistent with the bank's overall strategic and business plans, and adequate expertise should be employed to operate and maintain such systems. It is therefore imperative that e-banking risks be managed as part of a bank's overall risk management process. The levels of risk assumed need to be consistent with the bank's overall risk tolerance, and not exceed its ability to manage and control risks.

The Central Bank of Barbados expects that bank management and staff will ensure that they possess the pre-requisite knowledge and skills necessary to understand and effectively manage e-banking risks regardless of how a system is developed or operated. Controls should take into account the institution's risk exposure.

The party in the best position to control the risks, whether in-house or outsourced, should accept responsibility for controls. Essentially, the controls necessary to manage

risk effectively will differ depending on the degree of risk posed, the design and operation of the e-banking system.

2.2 Approach

Risk mitigation should include (i) controls (ii) security policy and awareness programmes. Banks' management will be expected to manage the varying levels of risks posed by electronic transactions.

(i) Controls: **A security programme should be in the form of a bank-wide implementation of physical and data security controls to protect critical information and physical assets from internal or external compromise.**

E-banking systems require effective and reliable controls to maintain data integrity, ensure customer privacy, and protect the bank's computer and telecommunications systems from unauthorized intrusions, misuse, or fraud.

A single password without an accompanying card, key or combination of passwords, may not provide sufficient authentication of bank customers. Banks should use a combination of access, authentication and other security devices to create a secure e-banking environment. These should typically include passwords, firewalls, and encryption, among others.

Security controls[4] that govern network and data access, user authentication[5], transaction verification, and virus protection should be developed. In general, banks should authenticate the identity of e-banking customers prior to accessing personal account information or engaging in electronic transactions. Due to security and risk management concerns associated with specific e-banking systems, banks require stronger authentication methods than those provided by most traditional systems. *(See Appendix IV).*

4 Access controls allow verification and enforcement of a user's authorized right to access a bank's network, applications and data.

5 Authentication is the process of determining whether PC banking system users are accurate.

(ii) Security Policy and Awareness Programs: The security programme should comprise policies, procedures and controls necessary to safeguard the bank's information, define individual responsibilities, and describe enforcement, contingency and disciplinary actions following non-compliance. A comprehensive information security policy should outline a proactive and ongoing program incorporating three components:

- *Prevention*:

  Prevention measures usually include sound security policies, well-designed system architecture and properly configured firewalls backed by strong authentication programs. Typically, there are two categories of prevention measures: (a) vulnerability assessment tools[6]; and (b) penetration analyses[7].

- *Detection*:

  Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm. Alarms Detection measures involve the analysis of available information to determine whether or not an information system has been compromised, misused, or accessed by unauthorized individuals. alert the financial institution or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

6 Vulnerability assessment tools generally involve a system to proactively detect known vulnerabilities.

7 Penetration analysis involves an independent party testing an institution's information system security to identify - and possibly exploit - vulnerabilities in the system.

- *Response*:

  Banks should have an effective incident response programme outlined in a security policy that prioritises incidents, discusses appropriate responses through appropriate channels, and establishes reporting requirements.

2.3 Specific Guidance

Banks' management should establish an effective planning process to implement and monitor systems. Overall, through the various controls, programmes and policies, banks should seek to:

- **Adopt effective and reliable security controls for electronic banking, that integrate into the bank's overall security programme, including system-wide access controls, user authentication, encryption, transaction verification, and virus protection controls;**

- **Update "know-your-customer"[8] and suspicious activity reporting (SAR) considerations consistent with appropriate identification, authentication and transaction verification methods;**

- **Implement policies and controls according to the sensitivity and importance of data;**

- **Update plans, policies and systems regularly, removing key elements of sensitivity risk assessments;**

---

8 Note an updated version of Central Bank of Barbados' "Know-your-customer" guidelines issued on March 2001 which updated those issued in 1996.

- **Establish effective risk monitoring processes, with specific emphasis on security and performance monitoring, as well as audit/quality assurance reviews;**

- **Develop e-banking systems in tandem with regularly tested bank contingency, business continuity and customer service plans;**

- **Identify expertise, as well as address staffing needs, and training requirements;**

- **Monitor developments and changes in relevant consumer and banking laws, rules and regulations, and take adequate measures to ensure compliance;**

- **Ensure that customer/depositor education is sufficient for the optimal use of the authentication and transactional functions of e-banking;**

- **Assess whether e-banking products offered may be subjected to unexpected assertions of jurisdiction by courts, agencies and taxing authorities in new geographic, product, or service markets; and**

- **Assess the legality of customer transfers and ensure that all relevant information has been included.**

SECTION 3

3. ELECTRONIC PAYMENT SYSTEMS

Electronic banking capabilities have changed the framework of payment systems, but banks will continue to participate in a number of dynamic roles, ranging from issuer to transaction authoriser and processor. Because of this, attention must be paid to the risks and possible mitigation techniques with respect to the payments system.

3.1 Criteria

In all cases, there must be trust in the participants that issue, process, and settle payments. This level of confidence in the process is crucial to a payment system's acceptance, and these factors have historically maintained the banking industry's central position within the payment system.

Payment systems are evaluated on a number of criteria, including:

- **User privacy;**
- **Transaction legitimacy, security, and non-repudiation;**
- **System dependability, efficiency, and cost; and**
- **Merchant acceptance and convenience.**

3.2 Structure

Payment systems can be broadly categorized according to process methodology, in addition to system components and structure. The combination of such attributes will determine - to a large degree - the systems' inherent risk. Importantly, risk will vary significantly depending on system implementation, administration, and the controls employed. In 1999, the Office of the Comptroller of the Currency (OCC) highlighted a number of characteristics consistent with an electronic payment system, many of which are currently relevant. These are highlighted in **Table 1**.

Table 1 also highlights the primary decision areas in developing a payment system. Software is not specifically included, since it serves principally to convert the decisions regarding components, methodology, and structure into an operative system. Indirectly therefore, software decisions are imbedded throughout the table.

Importantly, the sub-categorisations in **Table 1** do not necessarily present solutions or decisions. In many ways, decisions run along a continuum, such as the degree of security or system integration.

3.3 Specific Risks and Concerns

In addition to these unique risks, traditional risks customary to banking activities are also present, including natural disasters, system attacks and participant failures. Highlighted below is a summary of the risks and concerns that are most pronounced under an electronic payment system at each stage of operations.

Issues and Concerns During the Planning and Implementation Stage

- **The use of inadequate decision processes while considering, planning, and implementing electronic capabilities;**
- **The impact of technology cost and pricing decisions on financial position;**
- **The implications of e-banking on global activities;**
- **The possibility of system design and capabilities not meeting customer demands; and**
- **The implications of increasing competition from or the involvement with non-financial entities.**

Issues and Concerns in Developing Operating Policies and Procedures

- **The possibility of managerial or technical incompetence relative to electronic activities;**
- **The likelihood of existing controls not adequately protecting confidential electronic information; and**

- **Existing policies and procedures not addressing the transaction speed and broad reach of electronic channels.**

Audit

- Audit trails may be more difficult in electronic systems.

Legal and Regulatory Issues and Concerns

- **User privacy issues, since there is no specific legal statute in Barbados with reference to consumer privacy;**
- **The possibility of contingent liabilities resulting from user or participant claims;**
- **Uncertain legal jurisdiction with respect to taxation, criminal, and civil laws;**
- **With the increasing use of the available technology, the nature of international commerce will change. Therefore, those offering services in participating jurisdiction will need to update their infrastructure in all firms in order to remain competitive or gain competitiveness;**
- **Uncertain regulatory environment (international financial services and other areas); and**
- **Uncertain acceptability of some electronic documentation/disclosures under various regulations.**

Administration Issues and Concerns

- **The possibility of hardware and/or software failures or disruptions;**
- **A possible system and/or data base compromise;**
- **Inadequate system capacity;**
- **System obsolescence;**
- **Perceived difficulties in the administration of multiple standards and protocols;**
- **The inadequate protection of electronic communications; and**
- **Inadequate system security and controls.**

Issues and Concerns Related to Vendors and Outsourcing

- **Risks from reliance on vendor competence to perform critical functions, since internal controls may not extend to third party vendors;**
- **Weak system support among vendor group;**
- **The maintenance and administration of multiple inter-related systems; and**
- **The possible failure to monitor inter-relationships among multiple financial institutions, vendors or originators, and participants within a payment system.**

Notably, the effects of a system failure or compromise can rapidly extend beyond the interested parties. Furthermore, the reputational harm and lost confidence could seriously jeopardize the viability of the underlying payments system, especially for virtual banks. Therefore, comprehensive risk management programs are critical to identifying and responding to such incidents.

3.4 Risk Management

Risk management is the ongoing process of identifying, measuring, monitoring, and managing potential risk exposure. Consideration as it relates to the payments system, should be given to:

- **General supervision**: Close supervision should encompass the functions of planning and analysis, policies and procedures, accountability and authority, regulatory compliance and legal framework, human resources, and audit;
- **Transaction processing**: Management of transaction processing should emphasise user authentication, information integrity, non-repudiation of transactions, and data confidentiality; and
- **Systems administration**: As evidenced by resource requirements, system security, system reliability and contingency planning, system capacity, outsourcing policies, and systems update control.

There are some risk management functions, which have more specific relevance for electronic banking. These include – among other things - alterations to strategic planning and feasibility analysis, incident response and preparedness, and internal controls. Generally, traditional risk management techniques can be applied to electronic delivery and payment systems.

Prior to an incident, individuals should be formally appointed and empowered with sufficient latitude and authority to respond in the event of a breach. An assessment of the risks posed by each system must be made. Here, the principal departments, resources, activities, and constituencies that can be potentially impacted upon by a problem must be accounted for**.**

3.5 Specific Guidance

Participants should:

- **Engage in strategic planning and feasibility analysis[9];**

- **Review or implement management supervision, internal controls, and operating policies and procedures;**

- **Implement sufficient audit and testing with adequate incident response and preparedness plans;**

- **Engage in vendor due diligence, and vendor/internal support teams, with ongoing reviews of technological developments and capability enhancements;**

9 Feasibility analysis is the process of determining the likelihood that a proposal will fulfill specified objectives. The analysis should begin at the point an opportunity is identified, such as e-banking, and continue through deployment. Specifically, each opportunity should be analyzed in three stages: (1) Study;

- **Implement physical and system access controls, including on-site security, system passwords, firewalls, encryption, and intruder detection mechanisms aimed at repelling unauthorised intruders;**

- **Utilize authentication controls to preserve the integrity of the data. Such controls include acknowledgment, computerized logs, digital signatures, edit checks, and separation of duties, aimed at maintaining adequate audit trails and the accuracy of data;**

- **Require appropriate acknowledgment controls necessary to ensure the completeness of transactions. These include batch totaling, sequential numbering, one-for-one checking against the control file, adherence to protocols, anti-virus software, offsite backup, and contingency planning; and**

- **Ensure that knowledge is transferred among employees and customers and ascertain that legal opinions and reviews in areas of uncertainty regarding electronic banking activities/electronic money are conducted.**

(2) Design and Development; and (3) Operation, during which the system is operated and maintained.

SECTION 4

4. E-BANKING AND EXAMINATION PROCEDURES

The Central Bank will also be making the necessary changes to the conduct of the Central Bank of Barbados' (CBB) audits as electronic banking develops in Barbados. Therefore, examinations will require an even more risk management-based approach. Examinations that involve banks with electronic transaction capabilities will require specialists who are able to complete technical, as well as safety and soundness audits. The CBB proposes to expand its institutional capacity to perform these functions or draw on third-party sources that can provide unbiased analyses. Essentially, CBB examiners will evaluate an institution's overall effectiveness in controlling the broad risks inherent in electronic delivery systems.

In the absence of any reliance on third-party audits, pre-examination planning efforts will, for example, include a review of the bank's web site to obtain a preliminary indication of the level of sophistication of its e-banking capabilities. Examiners will complete safety and soundness electronic banking examination procedures for each system deployed, along with some determination of the appropriate treatment for each system.

> *Despite the fact that consultations with information systems specialists and electronic banking experts have been incorporated into the safety and soundness electronic banking guidance at critical junctures, banks are reminded that the levels of access and speed can magnify risk in an electronic environment. This therefore warrants enhanced vigilance.*

4.1 Review of Operating Policies and Procedures

Electronic capabilities can significantly change the character of a bank's business or enable it to introduce new products, services, and delivery channels. Policies, procedures, and other operating guidelines must keep pace with this new environment,

either through updates of existing documents or through the development of appropriate standards. Examiners of the Central Bank of Barbados will seek to ensure that:

(i) There are adequate policies and procedures relating to risk management which involve some element of a segregation of duties;

(ii) An effective security program has been implemented with the appropriate communication on policy, procedures, and practices, with the necessary support from the bank's directorate;

(iii) Following its assessment of critical and sensitive matters, all inventory systems, applications and data sources, are applicable;

(iv) The development, documentation and co-ordination of appropriate policies, procedures, and practices, have been implemented;

(v) There has been adequate education for both employees and customers regarding the use of bank electronic platforms;

(vi) Banks ascertain the completeness of each system in meeting minimum standards required for completing and enforcing legal documents and regulations;

(vii) **Guidelines for access levels, exception reporting, and record retention will be established and monitored and updated on a regular basis; and**

(viii) **Irrespective of whether electronic capabilities are developed in-house or acquired through a service provider, the bank retains the obligation to ensure minimum standards of operation.**

TABLES

Table 1: Characteristics of Electronic Payment Systems

System Components:	• System hardware (i.e., PC, card reader, ATM, etc.) • Chip versus magnetic strip technology • Card versus computer-based systems
Process Methodology:	• Batch versus real-time processing • Online versus offline access
System Structure*:	• Legal currency versus branded (proprietary) value • Single versus multiple currency • Debit versus stored value based systems • Open versus closed systems * • Reloadable versus single use systems • Controlled versus secured access • Single versus multiple purpose • Integrated versus stand alone systems • User anonymity • Payment mechanics (buyer and seller interaction) • Payment system settlement (processing) • Transaction size (micro or large-dollar payments) • Geographic reach

**With respect to payment systems, open systems are characterized by broad geographic presence and acceptance by a large number of merchants or programs. Closed systems generally involve a smaller geographic presence and/or a single or limited purpose use.*

Source: Office of the Comptroller of the Currency (1999)

APPENDIX I

Risk Management of Outsourced Technology Services

Banks need to understand the risks associated with outsourcing arrangements for technology services, and must ensure that effective risk management practices are implemented. Financial institutions increasingly rely on services provided by third parties to support an array of technology-related functions. While such outsourcing can help manage costs, obtain necessary expertise and improve services, it also introduces risks that banks and other financial institutions should address. In this context, it is therefore necessary to implement an appropriate and effective risk management process.

Following a complete risk assessment, management of each bank should evaluate service providers to determine their ability, both operationally and financially, to meet the bank's needs. Factors such as the third party's technical and industry expertise, operations and controls, and financial position should be considered when performing due diligence tests. Such needs, objectives and necessary controls should be communicated to the potential service provider.

Banks should also implement an oversight program to monitor third party controls, conditions and performance. In charting the performance of the service provider a financial institution should:

- **Adopt appropriate procedures for evaluating decisions to outsource e-banking systems;**

- **Conduct appropriate risk analysis and due diligence prior to selecting an e-banking service provider;**

- **Ensure the execution of periodic independent audits of outsourced operations;**

- **Assess the service by a regular report, documenting performance, as well as the speed of problem-solving and follow-up;**

- **Monitor the contract in the event of any compliance and revision needs;**

- **Assess the internal capacity necessary to evaluate and oversee outsourcing relationships;**

- **Implement necessary controls and reporting processes;**

- **Ensure that the responsibility for the administration of the service provider relationship should be assigned to personnel with appropriate expertise to monitor and manage the relationship;**

- **Ensure the presence of contingency plans, such as the availability of alternative service providers, costs and resources required if such a change becomes necessary; and**

- **Define performance expectations under both normal and contingency circumstances[10].**

10 Contingencies should address credible worst-case scenarios for providing continuity

APPENDIX II

Brief Overview of Digital Signatures and Certification Authorities (CAs)

All e-banking systems should be constructed to ensure that they interact with a valid database, and that no individual user has the authority to change their access privileges within the e-banking authorisation database. The certification authority – a third-party agent – offers such safeguards. A CA system involves the use of mainframe and personal computers, communications networks, and supporting software systems to provide electronic authentication services. The basic operational elements of a certification authority system are similar to an electronic banking system, with many possible configurations of computer software, hardware, and telecommunication links with its users.

Digital certificate systems, which represent one form of electronic authentication services, employ digital signatures that are created with public key cryptography. Although public key cryptography (PKI) - also known as asymmetric key cryptography - is not a new technology, it is relatively new to the financial services industry. Public key cryptography adds a layer of security beyond that of symmetric key systems by associating two keys or algorithms with the encryption/decryption process: a public and a private key. Although the public/private key pair is related functionally, the mathematical function associated with the public key is not identical to that function associated with the private key.

Electronic information transmitted under PKI technology generally ensures the content and sender of the information received has not been intercepted or altered. The private key is an algorithm known only to its owner; the public key is published for general use. Only the intended reader, the owner of the associated private key, would have the ability to decrypt and gain access to a message received. Message encryption is a separate software application. The CA system provides the digital certificate that formally links the identity associated with any given digital signature to the region's public key.

APPENDIX III

Online Privacy of Consumer Personal Information

The Central Bank of Barbados (CBB) appreciates the importance of information exchange over electronic media and the benefits for banks and consumers emanating from such exchanges.

Because the dramatic pace of technological change has enhanced the collection of diverse pieces of consumer personal information and increased the velocity of data transfer, the potential for personal information to be used in ways unwanted by consumers is likely to become a growing risk to financial institutions.

These guidelines promote the security and confidentiality of consumer records and information. They also attempt to point banks to protecting against any anticipated threats or hazards to the security or integrity of records, or any unauthorized use or access that would result in harm or inconvenience to the customer.

The CBB encourages financial institutions to maintain an awareness of emerging consumer online privacy concerns, and to take specific voluntary actions to address them. In particular, financial institutions should provide meaningful disclosures of privacy policies and information practices, which should then be effectively enforced. Consumer privacy concerns are being influenced by changes in the industry and technology. The CBB considers consumer privacy to be an important element of public trust, reputation and confidence in depository financial institutions, both internationally and domestically.

Consumers in a number of studies in the US have cited three primary concerns relating to privacy in an electronic environment. These are:

- How personal information is being collected;

- How the information is used by the collecting entity, particularly for purposes other than the original transaction; and
- Whether personal information is transferred to third parties, and for what purpose it has been transferred.

It is important that plans to deploy electronic systems include the consideration of the full range of implications for consumer privacy. In Barbados at present, there are no clear enforceable rules relating to consumer privacy, but breaches can potentially harm a bank's efforts at e-banking, thereby significantly impacting on a bank's overall condition. To do otherwise may impact the institution's compliance posture[11], and possibly result in consumer complaints or contingent liabilities through civil actions.

Banks should train staff about their responsibilities under the institution's privacy policies and information practices – some of which will be influenced by head offices in North America and Europe. They should also ensure that online privacy policies and information practices are consistent with the bank's policies for traditional transactions. Information practices can only be effective when accompanied by employee education, adequate internal controls, meaningful enforcement and redress. In crafting privacy policy there are a number of general principles that should be considered. These imply that there should be:

- **Notice to consumers about information and disclosure practices;**
- **Choice for consumers about the collection and the ability to restrict the use of such information;**
- **Security and accuracy of consumer information collected to protect against loss, unauthorised access, or misuse;**

11 Specific attention should be paid to the Fair Trading Commission and the proposed consumer protection legislation.

- **Access for consumers to information collected and the ability to identify and correct errors in a timely and inexpensive manner; and**

- **Enforcement and consumer redress to ensure compliance with the privacy policy and information practices and a means of recourse for an injured party.**

APPENDIX IV

Overview of Widely-Used Basic Security Safeguards

To protect against breaches, the basic security architecture in e-banking should include passwords, along with appropriate firewalls and encryption. Since breaches may result in serious reputational damage or financial loss, the bank should seek as quickly as possible to allay the fears of customers; who should also be directly informed of any substantial breach in an attempt to negate any potential repercussions and knock-on effects. These are highlighted below:

A. Passwords: **Banks should assign passwords or PINs (personal identification numbers) to users to control access to e-banking systems, and to ensure the integrity of passwords.** Banks should also assist by providing instruction on their proper use and protection. Specifically, management should consider the following password protection practices:

(i) *Minimum character length for passwords;*
(ii) *Use of alphanumeric passwords;*
(iii) *Periodic changes in passwords through automatic expiration;*
(iv) *Procedures for resetting user passwords and identification;*
(v) *Session controls that ensure automatic log-off during inactivity or after a set number of failed access attempts;*
(vi) *Prohibition of unencrypted password storage;*
(vii) *Encryption of passwords or PINs during transmission; and*
(viii) *Disallowance of automatic password save features.*

B. Firewalls: **Firewalls need to be based on the desired level of security as dictated by the bank's risk assessment and data classification efforts.** Firewalls are a combination of hardware and software to block unwanted communications flowing through a bank's network, while still allowing *bona fide* communications to pass.

C. Encryption: **Agreements between the bank and its customers should define the procedures for valid and authentic electronic communications between parties.** The levels and types of encryption should be based on the sensitivity of data or information being transmitted.

. The strength of current encryption techniques depends on a combination of three elements: a mathematical algorithm, key length, and the confidentiality of the key used to encode the message. These agreements should specify that the parties intend to be bound by communications that comply with these procedures. Encryption transforms data into an unreadable format.

APPENDIX V

Some E-Banking Terms

C*ertification authority* (CA): Similar to a notary, engages in electronic authentication and confirms the identities of parties sending and receiving electronic payments or other communications.

Data Classification: The act of classifying, or "categorising" data and systems according to its sensitivity and importance.

Digital signature: A unique code, created by a software application that aims to confer a certain level of security on a communication.

Intrusion Detection Systems: Defined as computer-based systems that detect unauthorised access to the bank's systems and can be used to detect network activity or intrusions. Generally, IDS products use three different methods to detect intrusions. First, they can look for identified attack signatures[12]. Second, they can look for system misuse. Third, they can look for activities that are different from the users' or systems' normal pattern. Such "anomaly-based" products are designed to detect subtle changes or new attack patterns.

Penetration Testing: Regarded as the process of identifying, isolating, and confirming possible flaws in the design and implementation of all types of security controls. These tests simulate the probable actions of unauthorized and authorized access, since the tactics used by unauthorized users to infiltrate computer systems frequently change. However, penetration testing cannot conceive nor guarantee protection from all types of attacks.

Performance Monitoring: Techniques or surveillance that determine whether the electronic banking system is working as planned. Indicators should include system

12 Streams or patterns of data previously identified as an attack.

response times, system availability, categories of customer inquiries, problem resolution, estimation of capacity needs, traffic volume, and customer profiles performance problems.

Quality Assurance: An objective review of electronic banking systems that identify and quantify risk, in addition to detecting possible weaknesses in the bank's risk management system.

Repository: A database of active digital certificates for a CA system. The main function of a repository is to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages.

Virus Protection: Computer software that is intended to detect and in most instances remove any virus that has the potential to corrupt computer systems. Virus protection software is an important security control element in any operating computer system. This is a necessary element since firewalls may not detect viruses with any degree of accuracy.

Queries and concerns may be directed to:

Banking Analyst
Governor's Office
Central Bank of Barbados
P.O. Box 1016
Bridgetown
Tel: 246-436-6870 : Fax: 246-427-9559