GUIDELINES ON
RISK MANAGEMENT OF ELECTRONIC BANKING
(Issued under Section 49 of the Financial Services Commission Act, R.S.A. c. F28 as amended)

These guidance are directed toward the Boards of Directors and senior managements of licensees under the Banking Act, R.S.A. c. B11 (insofar as their obligations specified in the Anti-Money Laundering and Terrorist Financing Regulations, R.R.A. P98-1 (as amended) are concerned) and the Trust Companies and Offshore Banking Act, R.S.A. c. T60 (particularly offshore banks).

Electronic banking can be defined as the process through which customers may perform banking transactions electronically through networks and the internet via personal computers, laptops, tablets, mobile phones and other devices.

The Commission endorses the principles and recommendations in the Basel Committee on Banking Supervision paper entitled "Risk Management Principles for Electronic Banking" issued July 2003 (http://www.bis.org/publ/bcbs98.pdf) and, in particular, Principle 4 dealing with the appropriate measures to be taken by a licensee to authenticate the identity and authorization of customers with whom it conducts business over the Internet.

This guidance comprises – as Appendix I and II - the Executive Summary of the BCBS paper and the summarized principles. However, the attention of licensees' Boards of Directors and senior management is directed to the BCBS publication in its entirety, at the link identified in the previous paragraph.

Approved by the Board
Anguilla Financial Services Commission
18 February 2014

Appendix I

Risk Management Principles for Electronic Banking

Executive Summary

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

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

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

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

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

For a similar reason, the *Risk Management Principles* issued by the Committee do not attempt to set specific technical solutions or standards relating to e-banking. Technical

solutions are to be addressed by institutions and standard setting bodies as technology evolves. However, this Report contains appendices that list some examples current and widespread risk mitigation practices in the e-banking area that are supportive of the *Risk Management Principles*.

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

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

Board and Management Oversight

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

Security Controls

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

Although customer protection and privacy regulations vary from jurisdiction to jurisdiction, banks generally have a clear responsibility to provide their customers with a level of comfort regarding information disclosures, protection of customer data and business availability that approaches the level they can expect when using traditional banking distribution channels.

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

Legal and Reputational Risk Management

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

Appendix II

Principle 1:
The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.

Principle 2:
The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.

Principle 3:
The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

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

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

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

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

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

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

Principle 10:
Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

Principle 11*:*
Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.

Principle 12:
Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.

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

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