AN INVESTIGATION OF THE RISK MANAGEMENT PRACTICES IN ELECTRONIC BANKING OF COMMERCIAL BANKS IN BARBADOS

Anthony Wood and Shane Butcher

The University of the West Indies, Cave Hill Campus

ABSTRACT

The financial services industry has undergone significant changes to its landscape. One salient feature has been the widespread adoption of technology in the banking industry. Banks have chosen to leverage information technology as the medium through which their numerous products and services may be accessed by their clients. This decision has resulted in a reduction of traditional brick and mortar branches in favour of Digital Financial Services (DFS) such as electronic banking. Within Caribbean banking this trend is noticeable due to the major operational restructuring which has resulted in a continuously shrinking footprint by major banks.

In 2002 the Central Bank of Barbados (CBB) provided an overview of the state of electronic banking in Barbados. They highlighted the fact that its usage had grown exponentially and had progressed from automatic teller machines (ATMs) to include telephone banking, electronic funds transfer (EFT) and point-of-sale purchases. Subsequent to this overview, commercial banks in Barbados have developed their electronic banking capabilities to offer E-Commerce solutions to many of their clients.

Utilising the CBB categorisation of electronic banking capabilities, Barbados' electronic banking climate may be classified as Level 3 which indicates a "fully transactional information transfer system". This classification embodies the highest level of functionality and equally high levels of exposure to risks. The Basel Committee on Banking Supervision (BCBS), recognising the need to address risks associated with the technologically advanced characteristics of electronic banking, developed fourteen risk management principles. The objective of this paper is to provide an empirical assessment of the risk management practices in electronic banking of commercial banks in Barbados. An electronic banking risk management index which measures the level of compliance with the principles is created. The instrument used for measuring the level of compliance is derived from the BCBS Risk Management Principles for Electronic Banking (2003). This paper represents the first such effort in the Caribbean and therefore adds to the sparse literature on risk management in electronic banking in the Caribbean context.

The results indicate that the commercial banks are highly compliant with the electronic banking principles. The index ranges from 76 to 100 on a scale of 0 to 100 in ascending order of good risk management practices for electronic banking. The findings should be of interest to many persons, including top management, shareholders and other stakeholders, regulators and future researchers.

Keywords: Barbados, Commercial Banks, Electronic Banking, Electronic Banking Risk Management Index, Risk Management Principles

JEL Classification: G21, G32.

Corresponding author: Anthony Wood; Email: Anthony.wood@cavehill.uwi.edu

1. INTRODUCTION

The financial services industry has undergone significant changes to its landscape. One salient feature has been the widespread adoption of technology in the banking industry. Banks have chosen to leverage information technology as the medium through which their numerous products and services may be accessed by their clients. This decision has resulted in a reduction of traditional brick and mortar branches in favor of digital financial services (DFS) such as electronic banking. Within Caribbean banking this trend is noticeable due to the major operational restructuring which has resulted in a continuously shrinking footprint by major banks.

Electronic banking may be seen as process innovation (Corrocher, 2002) since it strategically achieves operational efficiency through the reduction and control of costs. Users have maximized convenience, since they may now engage in activities such as the transfer of funds, bill payments and electronic commerce at their leisure whilst banks enjoy enhanced productivity and cost-effectiveness. In 2002 the Central Bank of Barbados (CBB) provided an overview of the state of electronic banking in Barbados. They highlighted the fact that its usage had grown exponentially and had progressed from automated teller machines (ATMs) to include telephone banking, electronic funds transfer (EFT) and point-of-sale purchases. Subsequent to this overview, commercial banks in Barbados have developed their electronic banking capabilities to offer E-Commerce solutions to many of their clients.

Utilizing the CBB's categorization of electronic banking capabilities, Barbados' electronic banking climate may be classified as Level 3 which indicates a "fully transactional information transfer system". This classification embodies the highest level of functionality and equally high levels of exposure to risks. Indeed, the extant literature has shown that while there are many benefits arising from electronic banking, there are also significant risks associated with this innovation (Basel Committee on Banking Supervision (BCBS), 1998, 2002; Schaechter, 2002; Solanki, 2012).

The BCBS, recognizing the need to address risks associated with the technologically advanced characteristics of electronic banking, developed fourteen risk management principles. The objective of this paper is to provide an empirical assessment of the risk management practices in electronic banking of commercial banks in Barbados. An electronic banking risk management index which measures the extent of compliance with the principles is created. The instrument used for measuring the level of compliance is derived from the BCBS Risk Management Principles for Electronic Banking (2003). This paper represents the first such effort in the Caribbean and therefore adds to the sparse literature on risk management in electronic banking in the Caribbean context.

The results indicate that the commercial banks are highly compliant with the electronic banking principles. The index ranges from 76 to 100 on a scale of 0 to 100 in ascending order of good risk management practices for electronic banking. The findings should be of interest to many persons, including top management, shareholders and other stakeholders, regulators and future researchers.

The remainder of this paper is structured as follows: section 2 reviews the relevant literature; section 3 presents an overview of the Barbadian commercial banking industry; the methodology is discussed in section 4 whilst the findings are presented and discussed in section 5; concluding remarks and areas for future research are contained in the final section.

2. LITERATURE REVIEW

2.1 ELECTRONIC BANKING EXPLAINED

The BCBS (1998, p.3) defined electronic banking as "the provision of retail and small value banking products and services through electronic channels". Similarly, Driga and Isac (2014) viewed electronic banking as the computerized conveyance of new and customary banking services and products. Banks are therefore able to disseminate services and data to their customers over an advanced information platform which permits usage of intelligent devices.

Electronic banking is an innovation which may render the administrative competences of the traditional brick and mortar banks obsolete (Cheung and Liao, 2003). Banks have embraced the opportunities provided by the internet and technology-driven solutions to ensure a competitive position within the market. Technological advancements within the banking sector provide numerous benefits such as increased customer base, reductions in cost, improvements in the timeliness and quality of responses, stronger customer relations and communication, and enhanced opportunities for advertising (Garau, 2002). Banks offer electronic banking capabilities with varying levels of sophistication in an attempt to leverage trends such as the mass diffusion of mobile phones and easy access to the internet and computers (Boateng, 2006). This assertion was substantiated by Abbasi and Weigand (2017) who noted that the introduction of 3G and 4G internet, and increased usage of smartphones have amplified the demand for digital services.

Electronic banking's origins can be traced back to 1981 where major banks such as Chase Manhattan and Citibank offered basic services such as online bill payment and the viewing of statements. However, over the years it has evolved and includes a wide array of services such as automated teller machines (ATM), internet banking, mobile banking, virtual banking and electronic funds transfer. More importantly, electronic banking capabilities have evolved beyond the traditional lending, promotional, deposit and non-deposit activities. These capabilities have enabled new "electronic payment options" such as digital cash or money (Federal Deposit Insurance Corporation (FDIC), 1997).

2.2 ELECTRONIC BANKING CAPABILITIES AND RISKS

According to the BCBS (1998), two central facets of electronic banking are the type of delivery channels utilized and the method by which customers obtain access to the delivery channels. Delivery channels used are categorized as "closed or open" networks. Closed networks confine access since usage is restricted by membership governed by agreements. Conversely, usage of open networks is not limited by any such membership agreements; the internet is an example of an open network which may be accessed by any computer equipped with internet capabilities. Electronic banking is heavily dependent on networked environments (such as the internet) for delivery of its capabilities to users and while each network does not carry the same levels of risks, vulnerability, importance and sensitivity, BCBS (2003) noted that each banking institution

must ensure adequate risk management responses to electronic banking risks. The level of risks associated with electronic banking capabilities can be categorized by their level of functionality. Thus the FDIC (1997) described three categories:

Level 1- Information-Only Systems
This type of system allows access to publicly available information and the diffusion of non-sensitive electronic mail which aid general-purpose marketing endeavors by the institution. It is a one-way communication system where the information is provided via a standalone server or from a website hosted by a third party. Essentially, the bank is merely disseminating information electronically as opposed to utilizing the traditional print media which is more costly. Risks associated with this type of system are deemed low and take the form of vandalism or mutiny of the information originally disseminated (Monetary Authority of Singapore, 2008).

Level 2- Electronic Information Transfer Systems
This system, which is categorized as interactive, permits the transmission of electronic mail and messages deemed to be of a sensitive or confidential nature, between the financial institution (FI) and users. It is important to note that the transmission of information, data or files occurs between the FI's network and its proprietary databases, and risks are commensurate with users' access to the bank's internal network. Therefore, the interactive nature of this system highlights the importance of communication security in an open network such as the internet where information is transferred. There is always the possibility of line tapping and the intrusion on transmitted data by individuals for whom this information is not intended. Key support personnel within network operations may have access to extremely delicate data which is conveyed over the networks. Risks associated with data integrity, privacy and confidentiality have to be considered since the internet is "inherently insecure as information travels openly over a series of connected networks" (FDIC, 1997).

Level 3- Fully Transactional Information systems
These systems provide the capabilities of both the information-only systems and electronic information transfer systems. Additionally, they facilitate other banking services such as online account requests, the administration of funds amongst multiple accounts, bill payments and electronic payment systems. It is important to note that the capabilities provided in this level are facilitated by "interactive connectivity between the customer's computer or other device and the bank's internal network or data base" (FDIC, 1997). Level three therefore presents the greatest exposure to risks since it grants users the maximum functionality over a networked environment and provides a medium through which users may interact with a bank's database.

It is important to note that whether the electronic capability delivered is transactional, interactive or informational, the mere provision of such services via the internet or any other electronic medium exposes the bank to unique risks inherent with electronic delivery.

2.3 IDENTIFICATION OF RISKS

The Electronic Banking Group (EBG) of the Basel Committee on Banking Supervision prepared a report on risk management and supervisory issues due to electronic banking activities. A critical observation made was the fact that electronic banking capabilities did not give rise to new unidentified undocumented risks, but rather electronic banking intensifies and transforms

the traditional risks, therefore affecting the general risk profile of the bank. The EBG highlighted that strategic, reputational and operational risks, in particular, were amplified by electronic banking undertakings. Similarly, the BCBS (1998) and Schaechter (2002) noted that banks engaging in electronic banking activities would primarily face operational, reputational and legal risks. Risk effects are not experienced in isolation; a risk situation occurring in one area of an entity can and will create another risk situation, thus risks must be considered in unison (International Finance Corporation (IFC) and Mastercard, 2016).

Strategic Risk

Strategic risk is defined as risk of losses to an entity as a result of an unsuccessful business plan (IFC and Mastercard, 2016). The European Central Bank (ECB 1998, p. 44) defines it as "the risk that the strategic objectives of an institution, the business strategies developed and the resources devoted to achieving these objectives as well as the quality of its implementation might not be consistent". Strategic risk exposure is associated with factors such as economic trends, business models and competitive positions. Inadequate strategic choices by a bank in relation to the technology choices for delivery of a digital service can result in technology risk which can result in operational risk, fraud risk and ultimately reputational risk as the customer experience was paltry (IFC and Mastercard, 2016). Competition now transcends boundaries and clients not satisfied with services rendered may easily switch to another provider. The probability of a strategic risk situation grows since the provision of such digital services is heavily dependent on ever-changing technologies. As it relates to electronic banking, Schaechter (2002) advised of the significant costs related to the requisite technological investment for such projects. Furthermore, the timing of these technological investments is paramount as "up-to-date" and widely used technology must be acquired. This innovation and disruptive technology in markets expose companies to become victims of occurrences such as obsolete products and inadequate responses to rapidly changing business environs. Thus, Sokolov (2007) noted that a bank's strategy to provide or expand its digital services should be duly informed by comprehensive cost-benefit analysis, planning and implementation.

Operational risk

Operational risk is intrinsic in the daily administration of any entity providing digital financial services such as electronic banking, and it arises due to the probability of losses resulting from deficiencies in the system's integrity and reliability (BCBS, 1998). Thus, the ECB (1998, p. 44) defines operational risk as "the risk that deficiencies in internal controls and information systems might result in unexpected losses for the institution". The Federal Financial Institutions Examinations Council (FFIEC 2016, p.7) defines it as "the risk of failure or loss resulting from inadequate or failed processes, people, or systems". This risk is normally associated with internal and external events such as inadequate procedures and controls, information system failures and human error. In particular the reliability and integrity of the daily support systems for the execution, delivery and process management of these services must be protected by well fashioned and documented business procedures (IFC and Mastercard, 2016). As a result, security against internal and external breaches, system design and customer misusage are critical considerations (BCBS, 1998) due to the banks' central dependence on technology for dissemination of these services. With the advent of electronic delivery of financial services, the BCBS (1998) noted that with the proliferation of computer technology and various communication paths, controlling access to banks' accounting, risk management systems and

information became complex. Schaechter (2002) advised that operational risks related to electronic banking should be managed in the areas of security, data confidentiality, outsourcing, system availability, and data and system integrity. Security threats may be internal or external and unauthorized access to a bank's system utilizing "back doors, hijacking or spoofing" gives the perpetrators unauthorized access to confidential information, assets and liabilities, and disrupts information integrity and services (Schaechter, 2002).

The BCBS (1998) remarked that an entity's system design, implementation and maintenance contribute to operational risk. An inadequately designed system prevents optimal delivery of services and can threaten system availability. Here factors such as capacity planning, forecasts of transaction volumes, recovery and response, and outsourcing are considered. In the event that a bank does not have the capacity regarding its system to provide services, then it considers outsourcing. The reliance on outsourcing contributes to a bank's operational risks since there is the possibility of "operator execution errors, data entry errors, accounting errors, lack of reporting and negligence which contribute to loss of client assets" (IFC and Mastercard 2016, p. 28). Outsourcing offers the benefit of cost reduction, but threatens system availability, integrity and reputation. Customer misuse, whether intentional or unintentional, contributes to operational risk especially where there is the lack of necessary measures to verify transactions done. As a result banks may lose funds due to their inability to detect fraud (BCBS, 1998).

Reputational risk

This risk refers to the potential losses due to damage to the corporate image of a provider, partner or stakeholder resulting in the reduction or total lack of trust from clients (IFC and Mastercard, 2016). The ECB (1998, p.44) defines it as the risk "that the reputation of an institution might deteriorate following specific events". Banks providing electronic banking have to be especially wary since heavy reliance on outsourcing and electronic delivery of such digital services exacerbates the possibility of a reputation risk situation. Reputational risk is not a direct risk but given its nature, its effects can be severe and have lasting overall negative consequences on the organization and market alike. For example, issues experienced with the delivery of these digital services from one entity may affect the customer confidence in the market on a whole, impairing the bank's ability to create new relationships and manage current ones (BCBS, 1998). In the context of electronic delivery of these digital services, reputational risk situations arise due to paltry customer service experience where failure in technology hampers the ability to complete transactions and lack of connectivity prevents clients' uninhibited access to their funds. Other drivers of reputational risk are lack of transparency in policies, human error, fraud, limited avenues for client recourse and poorly managed call centers through which client inquires and complaints should be resolved. According to Schaechter (2002), a bank's failure to consistently provide secure, precise and timely services threatens its reputation. Furthermore, should operational risks situations involving system integrity, availability and data confidentiality arise consistently, long-term damage to the bank's reputation would occur.

Legal/compliance risk

This risk situation occurs as a result of the potential non-compliance with or the infringement of regulations and laws which dictate the parameters or recommended practices, ethical standards, legal rights and contractual obligations of parties involved in the provision of these services. The benefits inherent in the usage of these digital services, such as remote processing capabilities to

overcome geographic barriers, intensify this risk. Electronic banking renders traditional methods of detection and prevention of criminal activity insufficient and obsolete. Thus, any bank which offers electronic capability must comply with regulations, consumer privacy protection and disclosure laws or face serious legal ramifications.

Financial risk
Risks such as credit and liquidity are specifically related to the financial management of the service provider.

Credit risk refers to the potential situation where counterparties fail to settle the full value of their obligation when it becomes due. Credit risk becomes important since electronic banking capabilities enable the disbursement of credit electronically over geographic territories. The probability of a credit risk situation is intensified if the procedures of that institution are scant and are unable to conclude the applicant's credit worthiness. Further, banks which offer the popular capability of electronic bill payment are exposed to this risk if there is refusal to settle payment obligations.

Liquidity risk refers to the potential situation where the bank fails to meet its obligations as they become due and becomes insolvent. A bank offering electronic banking capabilities has to manage its assets and liability composition. Therefore, banks should closely monitor factors such as transaction patterns, average cash deposits, inflows, outflows, durations and general customer behavior.

2.4 RISK MANAGEMENT CHALLENGES

The Electronic Banking Group (EBG) depicted the rudimentary characteristics of electronic banking which pose challenges to risk management. They focused on the rapid rate of technological change which fuels innovation in products and services offered to customers. Traditionally, when the implementation and testing process for new banking products and services was lengthy banks were afforded the time to conduct in-depth tests. However, in today's financial market characterized by stiff competitive pressure, success is measured by a bank's ability to provide new business products and services within compacted periods such as three to four months (from conception to assembly). This endeavour to be market leaders, according to the EBG exacerbates management's challenge to guarantee that ample efforts are put into risk analysis, reviews of security and strategic assessment before implementation of new electronic banking capabilities.

The websites which facilitate transactional financial services, such as retail payment capabilities over the internet, are naturally designed to enable as much integration as possible with computer systems to permit "straight-through processing" of electronic trades. The rationale for straight-through automatic processing is the reduction of human inaccuracy and fraud, commonly experienced in manual procedures. Conversely, the usage of a fully automated process intensifies a bank's dependence on comprehensive system architecture, interoperability and operational scalability (BCBS, 2003).

The FDIC (1997) and FFIEC (2016) alluded to the many functions which banks are capable of undertaking. More importantly, banks without the capabilities to perform tasks such as

settlements may have to outsource to third party processors. Thus, electronic banking may increase a bank's dependence on associations with numerous unregulated third party processors and their technical prowess, therefore intensifying security and operational concerns.

The internet is omnipresent by nature and therefore is widely accessible throughout the world by unknown individuals. The ability of these individuals to route and access information through undisclosed locations with high tech ever-evolving wireless gadgets makes it paramount for providers of electronic banking (and electronic money) capabilities to consider "security controls, customer authentication techniques, data protection, audit trail procedures, and customer privacy standards" (BCBS, 2003).

2.5 RISK MANAGEMENT FRAMEWORK

Fundamentally, every business is exposed to a variety of risks, both anticipated and unanticipated. It is paramount for banks that engage in the provision of electronic banking services to adopt a comprehensive risk management framework which enables it to adequately respond to present and future risk situations. An effective framework assists the board and senior management to mitigate potential losses and ultimately be proactive to risk management rather than reactive. This section reviews the relevant literature discussing the requirements of an effective risk management framework for banks providing electronic banking services. The key elements of the risk management framework are risk assessment, and management and control of risk.

Assessment of risks

The assessment of risks involves critical steps and within the context of electronic delivery is an iterative process. The first step is the identification and enumeration of risks associated with the delivery of such digital services. This enables the board and senior management to identify threats and vulnerabilities within the structure of the electronic delivery system comprising mechanisms such as hardware, software, system interfaces and applications, internal and external networks and human components (Monetary Authority of Singapore, 2008). According to the BCBS (1998), this should enable management to make rational and secure judgements about the probability and level of impact a risk situation may have. The IFC and MasterCard (2016) advised that the identification of risks should be done as early as possible to facilitate the development of adequate risk responses. The second step is the determination of the risk tolerance of the bank, both quantitatively and qualitatively by the board and senior management. These tolerance levels act as guides and benchmarks since a risk situation commensurate with a loss above the set tolerance level will be avoided or if below the threshold will be accepted.

Management and control of risks

A key way to control and manage risks is the establishment of quality, well-documented and communicated business procedures which add value to the customer's experience and alleviate risk situations. The IFC and Mastercard (2016) noted that numerous entities identify technology and governance as the primary causes of risk situations. However, the reality is that major occurrences of risk situations, such as fraud risk, in relation to digital financial services result from poor or non-existent business processes. Thus, areas which should receive adequate attention are security policy functions and processes, managing outsourcing risks, internal communication and business continuity planning.

Security policy functions and processes

The grouping of security principles, measures and procedures are known as the security policy functions and processes. These measures entail a combination of administrative and people management practices, software and hardware utilities which when adequately implemented, prevent and limit internal and external threats, protect the authenticity, integrity and confidentiality of systems, data and operating procedures (Monetary Authority of Singapore, 2008). Thus, the board and senior management must ensure proper development, implementation and dissemination of security policies and measures to all relevant staff. This conveys the bank's tolerance for risks as well as management's intent as it relates to protecting its electronic banking mechanism against intrusions. The bank may implement measures such as encryption which involves the use of cryptographic algorithms that mask data by converting it into a cipher which is not usable by unauthorized parties. Other measures such as firewalls, passwords, virus protection and employee screening procedures are options.

Certain security principles such as never alone, segregation of duties and access control should be observed by banks providing digital financial services like electronic banking. Never alone states that acute and complex functions such as the arrangement of network security, installation of systems, administration of operating systems, firewalls and cryptographic keys should either be jointly performed or if performed by one employee, should be immediately checked by another individual. Segregation of duties is seen as a technical approach which guarantees the implementation of adequate checks and balances to guard against failures of controls, opportunities for fraud and maladministration of funds. Duties such as the design and development of electronic delivery system, database management, data security and the management of access control should not be executed by any single employee or group of employees and should be subject to job rotation. Access control follows on from the segregation of duties principle since it too requires that access not be granted to an individual based on their rank within the organization but based on their job responsibility and need to complete mandated tasks. Care should be taken to prevent simultaneous access to critical systems such as data files or system recovery components and ultimately access should be granted for a defined purpose and time.

Management of outsourcing risks

Banks are known to outsource some of their operations for reasons such as financial efficiency and economies of scale. However, the bank's obligation and liability of controlling risks is not relinquished to the third party provider due to outsourcing. The due diligence of the third party should be performed to obtain information such as capacity, dependability and financial position. Written contracts which govern and clarify obligations and responsibilities of the parties involved must be agreed upon and enforced. These contracts should also include a clause which speaks to potential changes in third party providers should they fail to provide adequate levels of service. Outsourcing arrangements may require the bank to share sensitive information with its partner. Thus, contracts between these parties must ensure compliance with regulations of banking secrecy which require the protection of confidential customer information.

Internal communication

Internal communication is fundamental to managing and controlling risks, and should occur amongst the board, senior management and all key individuals involved within risk areas.

Operational, legal and reputational risks may be controlled when senior management demonstrates to key personnel how the provision of electronic banking is aligned to the overall goal of the bank. Conversely, technical employees should communicate to senior management any flaws within the system (BCBS, 1998). Banks are said to increase their capability to control risks when they readily disseminate all documentation about policies and procedures to their staff. It is therefore recommended that senior management implements a corporate policy which mandates employees to constantly train and educate themselves to keep abreast of changing technology.

Business Continuity Planning

Business continuity planning is essential to managing and controlling legal and reputational risks associated with disruptions in the delivery of electronic banking services to customers. The computer system is not immune to failure and thus disruptions in service delivery may occur at any time. Therefore, it is important that the board of directors and senior management ensure the creation, maintenance and testing of a continuity plan which establishes the course of action to be followed during disruptions. The BCBS (1998) stated that such a plan should cover aspects such as the recovery of data, alternative capabilities for data processing, emergency staff complements and customer services support. Plans should also address the bank's reliance on external hardware and software suppliers, internet service and telecommunication providers. The IFC and MasterCard (2016) advised that continuity plans should address damage to physical assets, hardware failure and the servers which host DFS applications. Furthermore, offsite storage of customer data to mitigate risks of losing customer data due to theft or human error should be addressed in the continuity plan.

3. OVERVIEW OF BANKING SECTOR IN BARBADOS

Barbados' banking industry conforms to the theoretical requirements of oligopoly: only a few firms in the industry so that the actions of one can affect the profits of another; bank deposits and loans are homogenous commodities and the number of banks is restricted by barriers to entry like the dominant position of established banks and financial regulations (Wood, 2012). Commercial banks dominate the financial system, accounting for 53 percent of total assets; followed by insurance companies with 15 percent; credit unions and pension funds with 9 percent each; mutual funds with 8 percent; and finance and trust companies with 6 percent (Central Bank of Barbados, 2017). Commercial banks also dominate the financial system in the areas of deposits and lending. Services provided by commercial banks include commercial, corporate and personal loans, mortgages, treasury, trust, capital markets investments and brokerage.

Since 2002 the ownership structure of the banking sector has changed significantly through a series of mergers and acquisitions in the sector. At present there are five commercial banks licensed to operate in Barbados: the Bank of Nova Scotia, CIBC FirstCaribbean International Bank (a merger of Barclays Bank PLC and Canadian Imperial Bank of Commerce (CIBC)), First Citizens Bank (Barbados) Limited (formerly Bank of Butterfield), Republic Bank (Barbados) Limited (formerly the Barbados National Bank), and RBC Royal Bank (Barbados) Limited (a merger of Royal Bank of Trinidad of Tobago (RBTT) and Royal Bank of Canada). The mergers and acquisitions in the banking sector may have been in response to the increasing global

pressures and the desire of these multinational corporations to expand market share, and enhance competitiveness and efficiency (Wood and Brewster, 2016).

Barbados' regulatory system conforms to the international standards set by the Basel Core principles for effective banking supervision. This sector is also scrutinized every five years by the Financial Sector Assessment Program which in 2008 concluded that Barbados performed well in relation to compliance with the Basel accords which set out requirements for credit, market and operational risks. Supervision of the banking sector is the responsibility of the Bank Supervision Department of the Central Bank of Barbados (CBB). It utilizes off and onsite inspection to monitor and report on the activities of all authorized financial institutions, ensuring that activities are in compliance with legislation. More importantly, the CBB which is responsible for the stability and further development of Barbados' banking sector, has created the framework for the implementation of the Basel two accord and has introduced consolidated risk-based supervision and numerous documented supervisory procedures which improve cross-border supervision.

The banking industry has weathered the global financial crisis and local recession relatively well, with capital adequacy ratios remaining well above international guidelines and the statutory requirement of 8%. Furthermore, the banks maintained a strong liquidity position in the post crisis period (Wood and Brewster, 2016). The Central Bank of Barbados during 2013 reported that various stress tests were undertaken to determine the impact of credit risk on the capital adequacy of banks and the results indicated that the banks remained solvent even in the face of sizable shocks. In addition, contagion effects were assessed based on the interconnectedness of commercial banks as well as their exposures to other regions, and the results underscored the resilience of the banking system. The soundness of the Barbadian banking system was also documented by Ramsaran (2013) and Central Bank of Barbados (2017).

Though the banking system remained resilience during the challenging economic period, the harsh economic circumstances introduced higher levels of uncertainty in the economy and a greater level of risk aversion among the household and business sectors. The resulting impact was a decline in loan demand and supply, increase in loan delinquency and weakened credit quality, thus leading to decreased profitability in the banking sector. The return on equity, which experienced a sharp increase from 9.7% to 19.3% between 2005 and 2007, declined to 15.6% in 2009 and recorded a historic low of 5.9% in 2012. Similarly, the return on assets increased from 1.6% to 2% between 2005 and 2007; subsequent declines were recorded with the ratio reaching 0.8% in 2013 (Wood and Brewster, 2016).

3.1 EVOLUTION OF ELECTRONIC BANKING IN BARBADOS

Craigwell et al. (2005) noted that financial innovation within the banking sector of Barbados was not a new occurrence and highlighted that as early as the 1990's electronic banking technologies such as ATM's and debit cards were in use. The CBB (2002) substantiated this view and stated that forms of electronic banking consisted not only of ATM's (the most popular form of electronic banking then), but of telephone/voice recognition banking, point of sale purchases and electronic funds transfer. Wood and Brewster (2016) also noted the heavy investments in technology made by financial institutions in Barbados. It is important to note that neither internet banking nor e-commerce were offered in the early 90's to 2002 as banks lacked the

capital base, risk mitigation techniques and the sophistication of their international parent companies which offer such services. Another key factor mentioned in the Central Bank's (2002) report was the lack of enthusiasm and demand for internet banking since Barbados was widely regarded as having a cash-based culture. This lack of demand and enthusiasm for internet banking continued and was addressed by Robinson (2010) in a media report titled 'too little e-banking'.

Robinson and Moore (2011), based on survey evidence from 2008 and 2009, revealed that 31% of Barbadians used internet banking services, further substantiating that this service was under-utilized. In a more recent study which focused on the attitudes and perceptions of middle-aged bank users in Barbados towards innovative bank products, Wood and Brathwaite (2014) revealed the sporadic, occasional usage of internet and mobile banking, and highlighted that the Barbadian bank users exhibited low levels of awareness of electronic banking capabilities such as mobile banking. Furthermore, internet banking, of which most respondent were aware, was thought to be under-utilized due to privacy and security concerns. Nevertheless, the electronic banking environment in Barbados continued to evolve since 2002 and more capabilities were introduced by banks.

In 2003 Scotia Bank disseminated internet banking capabilities to the Barbadian public and later introduced mobile banking in 2010. Banks also upgraded their system capacities to provide electronic commerce and this venture was supported by legislation such as the Electronic Transactions Act (2000) which legitimized digital transactions as the equivalent of physical paper transactions; the Computer Misuse Act (2005) and the Data Protection Bill (Walcott, 2007). Electronic money was also introduced by Bitt, a financial technology company in February 2016. Barbados' electronic banking environment can be said to have adequate capabilities since they are well documented on the websites of the various banking institutions. Thus, the challenge for banks is to increase awareness, usage and ultimately trust of innovative bank products which may be achieved if banks are more proactive at educating clients of the features, benefits, security measures and risk management processes (Wood and Brathwaite, 2014).

4. RESEARCH METHODOLOGY

The paper examines the risk management practices relating to electronic banking of commercial banks in Barbados. An empirical assessment of the extent to which commercial banks in Barbados comply with the fourteen electronic banking principles provided by the Basel Committee on Banking Supervision (BCBS) is undertaken. The methodology employed in the paper has features similar to studies undertaken by Sokolov (2007) and Abdou et al. (2014) on the commercial banking sectors of Estonia and the United Kingdom, respectively. To determine the level of compliance with the electronic banking principles of the BCBS, Sokolov (2007) collected information directly from the commercial banks through the use of questionnaires, while Abdou et al. (2014) adopted a quasi-quantitative approach utilizing semi-structured interviews and a questionnaire which applied a Likert scale to measure the extent to which respondents believed principles were adhered to. However, this paper seeks to improve construct validity and by extension the measurement of adherence to principles via the use of a compliance index.

4.1 ELECTRONIC BANKING PRINCIPLES

Previous studies conducted by the Basel Committee and the Electronic Banking Group (EBG) highlighted that electronic banking capabilities are inherently beneficial and risky. As a result, the Basel Committee in their 2003 report developed and disseminated 14 risk management principles (Table 1) which sought to provide guidance to ensure safe and sound electronic banking practices. They fall under the three broad categories of board and management oversight, security controls, and legal and reputation risk management.

Board and Management Oversight - principles 1 to 3

Principles 1 to 3 seek to provide the necessary guidance to ensure that electronic banking is provided within an effective framework. The strategic business decision to provide transactional electronic banking services and the establishment of management oversight for risks are the responsibilities of the board of directors and senior management. Any such decision must be well informed, documented and should include the necessary accountabilites, controls and policies which depict the manner in which such services shall be provided. The board and senior management are expected to comprehensively outline effective management oversight innitiatives. This involves the review and subsequent approval of internal control processes aimed at securing infrastructure which guard electronic banking systems against internal and external threats. Oversight management should also outline processes designed to manage risks associated with a bank's level of dependency on outsourcing key functions to third parties**.**

Security controls - principles 4 to 10

This set of principles requires that the rigor and content of the security control procedures implemented are purposefully managed and scrutinized due to the enhanced security risks associated with electronic banking. Therefore, the BCBS (2003) advised that aspects such as the effectiveness of authorization privileges, authentication processes, access controls, ample infrastructure security which protects data integrity and confidentiality by regulating usage of both internal and external entities, and audit trails of transactions should be focused upon. The principles also address areas such as the adequacy of information disclosure on a bank's websites to ensure that customers are duly informed of policies. Furthermore, the principles encourage banks to instill confidence in the level of service delivered.

Legal and reputational risk management - principles 11 to 14

These principles seek to protect the bank from legal, business and reputational risk situations. They emphasize that a bank providing electronic banking services should ensure adequate capability, continuity of business, communication strategies and incident planning to limit their liabilities associated with disruptions in service. This guarantees timely and consistent availability of systems to apease the high expectations of clients. Banks are also advised of the importance of effective event response tools to minimize the effects of unanticipated occurences such as internal or external attacks which retard the provision of electronic banking services.

Table 1

Board and Management Oversight

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.
2) The board of directors and senior management should review and approve the key aspects of the bank's security control process.
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.

Security Controls

4) Banks should take appropriate measures to authenticate the identity and authorization of customers with whom it conducts business over the internet.
5) Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.
6) Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.
7) Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.
8) Banks should ensure that the appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.
9) Banks should ensure that clear audit trails exist for all e-banking transactions.
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.

Legal and Reputational Risk Management

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.
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.
13) Banks should have effective capacity, business continuity and contingency planning processes to help ensure availability of e-banking systems and services.
14) Banks should develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal and external attacks, that may hamper the provision of e-banking systems and services.

Source: Basel Committee on Banking Supervision: Risk Management Principles for Electronic Banking (2003)

4.2 DATA COLLECTION AND ISSUES

The method of data collection used was the self-administered questionnaire (Appendix A) which is low-cost, quick to administer, not susceptible to interviewer bias and allows the respondent to complete the questionnaire at his/her convenience (Bryman, 2012). The questionnaire was distributed via email to the five commercial banks in Barbados which offer electronic banking capabilities during the period April and May 2018. The questionnaire was sent to persons directly involved with electronic banking within the commercial banks (Table 2).

Table 2

	Role	**Work Tenure**
Bank 1	Electronic Banking Systems Analyst	3 years
Bank 2	Manager Electronic Banking	4 years
Bank 3	Manager Electronic Banking	2 years
Bank 4	Business Banking Officer	4 years
Bank 5	Electronic Banking Officer	N/A

Source: Authors' compilation

The structure and content of the questionnaire were heavily informed by the 14 risk management principles and was partially guided by the previous study undertaken by Abdou et al. (2014). The questions addressed the three broad categories of issues outlined by the BCBS: board and management oversight, security controls, and legal and reputational risk management; and are therefore grouped under these headings. Furthermore, the structure of the questions was enhanced and the number of questions increased to more comprehensively capture the data. To elaborate this point, the category board and management oversight covered specifics such as staff competence requisite to the complexity of electronic banking. The category legal and reputational risk management covered key aspects such as business continuity, contingency planning and stress testing of systems. Thus, the structure and content of questions were modified to capture specific criteria under each broad category to ensure comprehensiveness. This specificity would lead to unbiased and comprehensive data collection.

The data-collection process was associated with a couple limitations. First, each bank offered electronic banking services with varying levels of sophistication as it relates to hardware and software utilized. Thus, the risk profile of each bank differed and the study was hindered in part by the dichotomous questions which did not allow for elaboration by a respondent if a bank did not adhere to a particular principle, but may have mitigated risk via alternative means. Second, the study targeted the five commercial banks operating in Barbados; however responses were received from three, giving a response rate of 60%. Though it would have been ideal to have comprehensiveness in the data collection, we are of the view that the data collected should still increase our understanding of the risk management practices related to electronic banking in Barbados.

4.3 COMPLIANCE INDEX

The compliance of the banks with the risk management principles was measured via the construction of an index based on twenty-one elements (questions) within three categories. The questionnaire utilized dichotomous elements, thus requiring the respondent to say yes or no. A yes response is coded 1 which means the bank is compliant, otherwise 0. Dichotomous elements were used as a defense mechanism against disadvantages associated with self-administered questionnaires. Bryman (2012) noted disadvantages such as the inability to probe and prompt, resulting in greater risk of losing data; difficulty utilizing open questions within the questionnaire; the risk of partially answered questions and lower response rates. The use of dichotomous elements, according to Bryman (2012), reduces the efforts of and clarifies content of questions for respondents, thus bolstering the response rate and understanding of the questionnaire. The sub-indices are equally weighted to avoid bias and in consideration of the

lack of information on the quality of electronic banking risk management practice in banks operating in Barbados. Unweighted scores have the advantage of treating each sub-index with the same level of importance without making arbitrary or data-driven judgements (Black et al., 2017). The final score was derived by adding the product of the weight and average score of the sub-indices and multiplying by 100. A higher score is an indication of better adherence to risk management principles. The methodology employed to construct the compliance index bears similarities to those employed previously in studies which focused on measuring adherence to corporate governance principles (for example, Gompers et al., 2003; Black et al., 2006; Bebchuk et al., 2009).

4. PRESENTATION AND DISCUSSION OF RESULTS

The risk management compliance index and ranking of financial institutions are presented in Table 3 and the scorecard to the questionnaire appears at Appendix B. The index ranges from 76 to 100 on a scale of 0 to 100 in ascending order of good risk management relating to electronic banking. Two of the commercial banks (Bank2 and Bank3) achieved compliance scores in excess of the average of 90.

Table 3: Compliance Index

Financial Institution	Score	Ranking
Bank1	76	3
Bank 2	95	2
Bank 3	100	1

Source: Authors' compilation

The results indicate that commercial banks in Barbados display high levels of compliance with electronic banking principles. This level of compliance was considered by the respondents to be heavily influenced by the electronic banking examination procedures utilized by the Central Bank of Barbados (CBB) where examiners ensure that adequate policies, procedures, effective security and communication of policy are present. Furthermore, respondents point to the fact that commercial banks operating in Barbados are affiliates of large banking corporations with parent companies headquartered in Canada, and Trinidad and Tobago. These parent companies are highly experienced in the delivery of electronic banking services in their respective markets and this wealth of experience is therefore leveraged in the Barbadian market where these services are offered.

The scores of the sub-indices are presented in Table 4. The results show that the banks performed well overall. All banking institutions scored perfectly in the area of security controls. This result indicates the board's awareness of their responsibility to ensure that the necessary security controls (authentication, non-repudiation, segregation of duties, data and transaction integrity, audit trails and authorization controls) with the requisite rigor are present. The scores also confirm adherence to not only principles 4 to 10 but to principle 2 which states that the board is responsible for the establishment of comprehensive security controls. This level of compliance was heavily influenced by the periodic audits and daily remote monitoring of systems conducted by personnel located at the head offices of the banks in Canada, and Trinidad and Tobago. In addition these entities were subject to monitoring performed by international

agents such as MasterCard and Visa which issued severe monetary penalties for breaches. Respondents for each bank revealed that they utilized methods such as personal identification numbers (PIN's), digital certificates and passwords to authenticate and identify clients. However, these methods may be undermined by a client, for instance, sharing his/her password. Segregation of duties, the internal control which reduces operational and fraud risks was highlighted as an area which was heavily adhered to but was becoming increasingly difficult due to consistent retrenchment of staff.

Table 4
Electronic banking principle's sub-indices

Commercial Bank	Board and Management Oversight	Security Controls	Legal and Reputational Risk Management
Bank1	57	100	71
Bank2	100	100	86
Bank3	100	100	100
Mean	86	100	86
Minimum	57	100	71
Maximum	100	100	100

Source: Authors' compilation

Bank 1 scored lowest in the categories of board and management oversight, and legal and reputational risk management amongst the three banks. Non-compliance with principle 1 was recorded where the board failed to clearly establish the bank's risk appetite and adopts new technology without ensuring that staff's expertise is commensurate with the level of complexity of the electronic banking system. It was found that factors such as the inability of the board and senior management to meet consistently due to geographic differences, rapid changes in technology and intense competition which results in the demand for new innovative products were at the root of these deficiencies. This gives credence to the assertion that there is significant pressure on banks to provide new products in very short timeframes as it relates to electronic banking (BCBS, 2003).

Furthermore, there was no suitable contingency plan to contain, manage or minimize fallout from the occurrences of internal and external attacks. This therefore exposes the bank to serious legal and reputational risks since customer privacy, incident response and the bank's ability to maintain 24/7 availability of services are all threatened should a risk event occur. This contravenes BCBS (2003) which asserted that banks have a responsibility to ensure that business availability and protection of customer information for electronic banking should be at the same level in comparison to traditional banking mediums. The above-mentioned factors responsible for non-compliance with principle 1 along with continuous reductions in staff complements were said to be responsible for Bank 1's non-compliance with principles 13 and 14 relating to the periodic review and stress testing of the electronic banking system. Bank 2 was also non-compliant with principle 14, resulting in a sub-index score of 86 for legal and reputational risk management.

Non-compliance with principles 1, 13 and 14 reveals deficiencies in the areas of board and management oversight, and legal and reputational risk management. The CBB's guidelines (2002) stated that banks have a responsibility to identify expertise, staffing and training

necessities. Thus, it is recommended that the recruitment process be strengthened to ensure that banks hire persons with the requisite skills to handle the complexity of the electronic banking system or training scheduled to alleviate this deficiency. This recommendation should result in banks achieving compliance with principles 13 and 14 since banks would have staff with the required skills and capacity to ensure segregation of duties, stress testing and business continuity. Customer education is important in curtailing the sharing of confidential information such as PINs. Therefore, it is recommended that banks share clear and concise versions of their privacy policy and ensure that visible instructions against the sharing of passwords and PINS are on websites where transactions are performed.

The results of this study were compared with those conducted by Sokolov (2007) and Abdou et al. (2014). Both studies referenced the fourteen risk management principles set by the BCBS. Results from the former study concluded that banks in Estonia were compliant with the BCBS principles. Specifically, 92% of the respondents were of the view that their banks adhered to the principles relating to management oversight, 100% to those principles relating to security controls and 83% thought that their banks had effective business continuity plans to deal with legal and reputational risk. The latter study concluded that banks in the United Kingdom were compliant with the BCBS principles. This conclusion was substantiated with the following results. Out of a mean score of 5 for each category, the ranges were as follows: 3.91-4.17 (board and management oversight), 4.13-4.84 (security controls) and 4.35-4.88 (legal and reputational risk management). Similarly, the results of this study indicated high levels of adherence of banks in Barbados to the BCBS risk management principles.

This paper referenced the rudiments of risk management for banks engaged in the provision of electronic banking services. The reviewed literature not only identified and discussed the risks associated with the provision of these services, but outlined a framework comprising best practices which enable banks to manage and control these risks effectively. These practices included identification of vulnerabilities in hardware and software systems, segregation of duties, management of outsourcing risks, business continuity planning, and the quantitative and qualitative determination of risk tolerance by the board and senior management. The framework addressed key procedures which coincide with the content of the best practices captured under each category of the BCBS principles. For example, the framework addressed the determination of the probability and potential level of impact, and subsequent determination of the bank's risk tolerance. These processes coincide with the content (risk tolerance) captured under board and management oversight. The framework's processes captured under the management and control of risks, coincide with those captured under security controls. One can therefore compare the information collected through the questionnaire with the literature addressing the risk management framework to ascertain the extent to which banks operate in accordance with the best practices outlined. Thus, analysis of the scores of banks can be used as an indication of areas of strengths or weaknesses in the risk management framework. We can therefore conclude that banks in Barbados have relatively strong risk management frameworks for electronic banking. However, improvements are needed in the risk management frameworks of Banks 1 and 2 in the areas of assessment, management and control of risks with respect to the determination of risks and business continuity.

5. CONCLUSION AND RECOMMENDED AREAS FOR FUTURE RESEARCH

There is limited research on risk management practices in electronic banking in the Caribbean. This paper addressed that deficiency through the construction of an electronic banking risk management compliance index for commercial banks in Barbados using survey evidence obtained during the period April and May 2018. The results indicated that on average, the banks achieved a compliance level of 90%, with the scores ranging from 76% to 100% among the three banks. Such scores indicate that the banks were highly compliant with the Risk Management Principles for Electronic Banking established by BCBS in 2003. The main contributory factors to the high level of compliance were the rigorous examination procedures of the Central Bank of Barbados, wealth of experience of parent companies in the delivery of electronic banking services in their respective markets and monitoring by international agencies such as MasterCard and Visa.

With regards to the sub-indices, the banks achieved maximum scores in the category of security controls. Analysis of findings revealed that there were some deficiencies as principles 1, 13 and 14 were not adhered to by two of the banks. This exposes the banking institutions to risks associated with inadequate management oversight, business continuity, and legal and reputational fallout. More interesting were the causes of non-compliance which ranged from the inability of the board and senior management to meet consistently, rapid changes in technology, intense competition which results in the demand for new innovative products and retrenchment of employees. Recommendations to address such deficiencies included revamping the recruitment process, training of staff, customer education with regards to a bank's privacy policy and ensuring visibility of warnings against sharing PINs and passwords.

Though the study produced some interesting results, it can be extended in a few important ways. First, the research is based on a single country. Future empirical work on electronic banking can be conducted on a Caribbean-wide basis or may consider a panel of Caribbean and other developing or developed economies. Second, another important area of research is examining the relationship between electronic banking compliance and bank performance. Third, it is well accepted that electronic banking and electronic money capabilities contribute to the smooth functioning of retail payment systems. Thus, future research can be conducted in the area of risk management for those financial institutions which undertake roles such as settlement in the retail payment system. Such an empirical assessment should produce data which identifies the nature and complexity of operations, and risk management procedures which seek to mitigate operational, strategic, legal and reputational risks associated with the retail payment system.

REFERENCES

Abbasi, T. and Weigand, H. (2017). "The Impact of Digital Financial Services on Firm's Performance: A Literature Review." *Ithaca: Cornell University Library. (arXiv).*

Abdou, H., English, J. and Adewunmi, P. (2014). "An Investigation of Risk Management Practices in Electronic Banking: The Case of UK Banks." Banks and Bank System, Vol. 9, No. 3, pp. 19-31.

Basel Committee on Banking Supervision. (1998). "Risk Management for Electronic Banking and Electronic Money Activities." Bank for International Settlements BS/97/122, Basel, Switzerland.

Basel Committee on Banking Supervision. (2002). "Management and Supervision of Cross-Border Electronic Banking Activities." Bank for International Settlements, Basel, Switzerland.

Basel Committee on Banking Supervision. (2003). "Risk Management Principles for Electronic Banking." Bank for International Settlements, Basel, Switzerland.

Bebchuk, L., Cohen, A. and Ferrell, A. (2009). "What Matters in Corporate Governance." *Review of Financial Studies*, Vol. 22, No. 2, pp. 783-827.

Black, B., Jang, H. and Kim, W. (2006). "Does Corporate Governance Predict Firms' Market Values? Evidence from Korea." *The Journal of Law, Economics and Organization*, Vol. 22, No. 2, pp. 366-413.

Black, B., De Carvalho, A., Khanna, V., Kim, W. and Yurtoglu, B. (2017). "Corporate Governance Indices and Construct Validity." *Corporate Governance: An International Review*, Vol. 25, Issue 6, pp. 397-410.

Boateng, R. (2006). "Developing E-Banking Capabilites in a Ghanaian Bank: Preliminary Lessons." *Journal of Internet Banking and Commerce,* Vol.11, No.2, pp. 1-11.

Bryman, A. (2012). *Social Research Methods, 4th edition.* Oxford University Press.

Central Bank of Barbados. (2002). "Guidelines for Electronic Banking." Available at: *http://www.central bank.org.bb.*

Central Bank of Barbados. (2017). Financial Stability Report. Available at: http://www.centralbank.org.bb.

Cheung, M. and Liao, Z. (2003). "Challenges to Internet E-Banking,." *Communications of the ACM,* Vol. 46, No.12, pp. 248-250.

Corrocher, N. (2002). "Does Internet Banking Substitute Traditional Banking? Empirical Evidence from Italy." *Research Center on Innovation and Internationalization Processes CESPRI WP* No.34.

Craigwell, R., Moore, W. and Coppin, K. (2005). "Financial Innovation and Efficiency in the Barbadian Banking Industry." *Money Affairs,* Vol.18, No.2, pp. 83-100.

Driga, I. and Isac, C. (2014). "E-Banking Services - Features, Challenges and Benefits." *Annals of the University of Petrosani, Economics,* Vol.14, No.1, pp. 49-58.

European Central Bank. (1998). "Report on Electronic Money." *Postfach, Frankfurt am Main.*

Federal Deposit Insurance Corporation. (1997). "Electronic Banking - Safety and Soundness Examination Procedures." Federal Deposit Insurance Corporation, Washington, D.C.

Federal Financial Instituitons Examination Council. (2016). "FFIEC Retail Payment Systems (RPS)." Federal Financial Institutions Examination Council, United States of America.

Garau, C. (2002). "Online Banking in Transition Economies: The Implementation and Development of Online Banking Systems in Romania." *International Journal of Bank Marketing,* Vol.20, No.6, pp. 285-296.

Gompers, P., Ishii, J. and Metrick, A. (2003). "Corporate Governance and Equity Prices." *The Quarterly Journal of Economics*, Vol. 118, No. 1, pp. 107-156.

International Finance Corporation (IFC) and Mastercard Foundation. (2016). "Digital Financial Services and Risk Management Handbook." International Finance Corporation (IFC), Mastercard Foundation.

Monetary Authority of Singapore. (2008). "Internet Banking and Technology Risk Management Guidelines." Monetary Authority of Singapore, Sheraton Way, Singapore.

Ramsaran, R. (ed.), 2013. *The Financial Evolution of the Caribbean Community (1996-2008), 2nd edition.* Caribbean Centre for Money and Finance, Trinidad.

Robinson, J. and Moore, W. (2011). "Attitudes and Preferences in Relation to Internet Banking in the Caribbean." *SSRN Electronic Journal* 10.2139/ssrn.2848357.

Schaechter, A. (2002). "Issues in Electronic Banking: An overview." *IMF Policy Discussion Paper 02/06,* International Monetary Fund, Washington, D.C.

Sokolov, D. (2007). "E-Banking Risk Management Practices of the Estonian Banks." *Institute of Economics, Tallin University of Technology* No.156.

Solanki, V. (2012). "Risks In E-Banking and their Management." *International Journal of Marketing, Financial Services & Management Research,* Vol.1, Issue 9, pp. 164-178.

Walcott, P. (2007). "Evaluating the Readiness of E-Commerce Websites." *International Journal of Computers,* Vol. 1, Issue 4, pp. 263-268.

Wood, A. (2012). "The Development of the Barbadian Financial System: 1966-1990." *International Journal of Business and Social Science*, Vol. 3, No. 6, pp. 61-73.

Wood, A. and Brathwaite, N. (2014). "An Exploratory Study of the Perceptions and Attitudes of Middle-Aged Banking Users in Barbados Towards Innovative Financial Banking Products." *Academy of World Business, Marketing and Management Development Conference Proceedings,* Vol. 6, No.1, pp. 345-363.

Wood, A. and Brewster, R. (2016). "The Impact of the Global Financial Crisis on the Performance of Commercial Banks in Barbados." *Journal of Management and World Business Research,* Vol. 13, No.1, pp. 13-27.

Appendix A: Research Questionnaire

Please tick the appropriate box to indicate your answer.

Board and Management Oversight (Principles 1-3)

Statement	Yes	No
1) The Board of Directors and senior managers have established effective management oversight (policies and controls) over risks related to electronic banking activities.		
2) The Board of Directors and senior management have reviewed and approved critical aspects of the bank's security control process.		
3) The Board and senior management address risks that threaten the security and integrity of electronic banking systems.		
4) The Board and senior management has clearly established the bank's risk appetite as it relates to electronic banking.		
5) The Board and senior management only adopts new electronic banking technology and business if the bank has the necessary competence to manage associated risks.		
6) The Board and senior management ensures that management and staff's expertise is commensurate with the level of complexity of the bank's electronic banking system.		
7) The Board and senior management have established comprehensive due diligence and oversight processes to manage outsourcing and third-party relationships upon which electronic banking is dependent.		

Security Controls (Principles 4-10)

8) The bank takes appropriate authentication measures to validate the identity and authorization of customers with whom it conducts business.		
9) The bank utilizes transaction authentication methods which encourage non-repudiation (proof of integrity and origin of data) and fosters accountability for electronic banking transactions.		
10) The bank ensures that the appropriate controls are present to encourage adequate segregation of duties within electronic banking systems, databases and applications.		
11) The bank ensures that adequate authorization controls and access privileges are present for electronic banking systems, databases and applications.		
12) The bank ensures that appropriate procedures are present to guard the data integrity of electronic banking transactions, records and information.		
13) The bank ensures that clear audit trails exist for all electronic banking transactions.		
14) The bank ensures that appropriate measures which preserve the confidentiality of sensitive information transmitted or stored are present.		

Legal and Reputational Risk Management (Principles 11-14)

15) The bank ensures that its website provides adequate information to potential customers to enable them to make informed inferences about the bank's identity and regulatory status.		
16) The bank's website provides information such as the name and locations of the bank; contact information for service centers which handle disputes, complaints and suspected misuse of accounts.		
17) The bank uses appropriate procedures to ensure adherence to customer privacy requirements which apply to the specific jurisdiction where the bank offers electronic banking services.		
18) The bank informs customers of its privacy policies and privacy issues regarding the usage of electronic banking.		
19) The bank has effective capability, business continuity and contingency planning procedures to guarantee accessibility of its electronic banking systems.		
20) Electronic banking transaction processing capabilities are stressed tested and periodically reviewed.		
21) The bank has developed and implemented suitable contingency plans to manage, contain and minimize issues which arise from events such as internal and external attacks.		

Please utilize the space below for any additional comments which you may want to state.

_____
_____
_____
_____
_____

Name of the Bank: _____

Thank you for your valued contribution to this research.

Appendix B: Electronic Banking Scorecard

Statement	Max Score	Section weight	Bank 1	Bank 2	Bank 3
Board and Management Oversight	**1**	**33.3%**	**0.57**	**1.00**	**1.00**
1) The Board of Directors and senior managers have established effective management oversight (policies and controls) over risks related to electronic banking activities.			1	1	1
2) The Board of Directors and senior management have reviewed and approved critical aspects of the bank's security control process.			1	1	1
3) The Board and senior management address risks that threaten the security and integrity of electronic banking systems.			1	1	1
4) The Board and senior management has clearly established the bank's risk appetite as it relates to electronic banking.			0	1	1
5) The Board and senior management only adopts new electronic banking technology and business if the bank has the necessary competence to manage associated risks.			0	1	1
6) The Board and senior management ensures that management and staff's expertise is commensurate with the level of complexity of the bank's electronic banking system.			0	1	1
7) The Board and senior management have established comprehensive due diligence and oversight processes to manage outsourcing and third-party relationships upon which electronic banking is dependent.			1	1	1
Security Controls	**1**	**33.3%**	**1.00**	**1.00**	**1.00**
8) The bank takes appropriate authentication measures to validate the identity and authorization of customers with whom it conducts business.			1	1	1
9) The bank utilizes transaction authentication methods which encourage non-repudiation (proof of integrity and origin of data) and fosters accountability for electronic banking transactions.			1	1	1
10) The bank ensures that the appropriate controls are present to encourage adequate segregation of duties within electronic banking systems, databases and applications.			1	1	1
11) The bank ensures that adequate authorization controls and access privileges are present for electronic banking systems, databases and applications.			1	1	1
12) The bank ensures that appropriate procedures are present to guard the data integrity of electronic banking transactions, records and information.			1	1	1
13) The bank ensures that clear audit trails exist for all electronic banking transactions.			1	1	1
14) The bank ensures that appropriate measures which preserve the confidentiality of sensitive information transmitted or stored are present.			1	1	1
Legal and Reputational Risk Management	**1**	**33.3%**	0.71	0.86	1.00
15) The bank ensures that its website provides adequate information to potential customers to enable them to make informed inferences about the bank's identity and regulatory status.			1	1	1

16) The bank's website provides information such as the name and locations of the bank; contact information for service centers which handle disputes, complaints and suspected misuse of accounts.			1	1	1
17) The bank uses appropriate procedures to ensure adherence to customer privacy requirements which apply to the specific jurisdiction where the bank offers electronic banking services.			1	1	1
18) The bank informs customers of its privacy policies and privacy issues regarding the usage of electronic banking.			1	1	1
19) The bank has effective capability, business continuity and contingency planning procedures to guarantee accessibility of its electronic banking systems.			1	1	1
20) Electronic banking transaction processing capabilities are stressed tested and periodically reviewed.			0	1	1
21) The bank has developed and implemented suitable contingency plans to manage, contain and minimize issues which arise from events such as internal and external attacks.			0	0	1
Total Score	1	100%	0.76	0.95	1.00