EASTERN CARIBBEAN CENTRAL BANK

PRUDENTIAL STANDARD FOR ELECTRONIC BANKING

FOR INSTITUTIONS LICENSED

TO CONDUCT BUSINESS UNDER THE BANKING ACT

December 2022

TABLE OF CONTENTS

BANKING PRUDENTIAL STANDARD NO. 3 OF 2022

This prudential standard is issued by the Eastern Caribbean Central Bank (Central Bank), in exercise of the powers conferred on it by section 184 of the Banking Act[1] .

1.0 Commencement

This Prudential Standard shall come into effect on the 1st day of February 2023.

2.0 Interpretation

The following terms are defined for the purpose of these guidelines:

i. ***"Access Control"*** refers to the controlling of access to system and network resources. It allows authenticated users access to specific resources based on company policies and permission levels assigned to the user or user group. Access control often includes authentication, which proves the identity of the user attempting to log in.

ii. ***"Authentication"*** refers to the techniques, procedures and processes used to verify the identity and authorisation of prospective and established customers.

iii. ***"Authorisation"*** refers to the procedures, techniques and processes used to determine that a customer or an employee has legitimate access to the account or the authority to conduct associated transactions on that account.

[1] Anguilla Banking Act No. 6 of 2015;
Antigua and Barbuda Banking Act No. 10 of 2015;
Dominica Banking Act No. 4 of 2015;
Grenada Banking Act No. 20 of 2015;
Montserrat Banking Act No.15 of 2015;
Saint Christopher and Nevis Banking Act No. 1 of 2015;
Saint Lucia Banking Act No 3 of 2015; and
Saint Vincent and the Grenadines Banking Act No 4 of 2015

iv. ***"Biometric technology"*** refers to an automated view of physiological or behavioural characteristics used to identify and/or authenticate a person. Common forms of biometric technology include facial scans, finger scans, iris scans, retina scans, hand scans, signature scans, voice scans and keystroke dynamics.

v. ***"Board"*** means the Board of Directors or other body responsible for the management of a Licensed Financial Institution.

vi. ***"Central Bank"*** means the Eastern Caribbean Central Bank (ECCB) established under Article 3 of the ECCB Agreement.

vii. ***"Cryptography or cryptography technique"*** refers to the art of protecting information by encrypting it into an unreadable format.

viii. ***"Confidentiality"*** refers to the assurance that information remains private to a licensed financial institution and is not viewed or used by those unauthorised to do so.

ix. ***"Cross-Border E-banking Activities"*** is the provision of transactional on-line or telephone banking products or services remotely from a bank in the ECCU to residents in a country outside the ECCU where the bank does not have a licensed banking establishment. This therefore excludes international banks' delivery of e-banking products and services to their customers in different countries via their licensed bank branches or subsidiaries in those countries.

x. ***"Data Integrity"*** refers to the assurance that information that is in-transit or in storage is not altered without authorisation.

xi. ***"External Auditor"*** is an external auditor appointed under section 60 of the Banking Act, that is:

a. A person who is a member of a professional body of accountants which the Minister of Finance has specified by order published in the Gazette; or
b. Any other person approved by the Central Bank.

xii. ***"Identification"*** refers to the procedures, techniques and processes used to establish the identity of a customer when opening an account.

xiii. ***"Institution"*** means a financial institution licensed to conduct banking business under the Banking Act.

xiv. ***"Internet"*** is defined to include all related web enabling technologies and open telecommunications networks ranging from direct dial-up connections, the public World Wide Web, and virtual private networks.

xv. ***"Logical Access Control"*** refers to the ability to interact with data through access control procedures such as identification, authentication and authorization.

xvi. ***"Material or Materiality" refers*** to the measurement of the importance of the relevant information about an item or person, which has the potential to influence significantly the decisions of lenders, investors, and other users of the financial information. Materiality can be related to the nature, size, complexity, and implications of the information.

xvii. ***"Material Activities"*** in relation to a Licensed Financial Institution refers to:

a. Activities or services of great significance; that any weakness or failure in their delivery could have a significant effect on the institutions' ability to continue as a going concern, and or meet its regulatory responsibilities;
b. Key systems, activities or services without which; would inhibit an institution from delivering services to its customers;
c. Any activity which would have a significant impact on an institution's risk management; and the management of risks relating to these activities; and
d. Any other activities requiring authorisation from the Central Bank.

xviii. ***"Network Access Control"*** refers to a broad term for managing access to a network. It validates users logging into the network and determines what they can see and do. It also scrutinizes the health of the user's endpoints (computers or mobile devices).

xix. ***"Outsourcing"*** means to enter into a contractual agreement with a third-party service provider, where the service provider manages functions, business activities, processes or products that are or could be undertaken by the LFI.

The definition of outsourcing does not include purchasing[2] contracts or the engaging of consultants to provide technical advice on operations or to organize and establish a serve; however, the use of a service provide to manage or deliver that service would constitute outsourcing[3].

xx. ***"Officers"*** of an institution means:

a. chief executive officer, chief operating officer, president, vice president, branch manager, country manager, corporate secretary, treasurer, chief financial officer, chief accountant, chief auditor, chief investment officer, chief compliance officer or chief risk officer;
b. any other individual designated as an officer by its articles of incorporation or continuance, bye-laws or other constituent document, or resolution of the directors or members; or
c. any other individual who performs functions similar to those performed by a person referred to in paragraph (a), whether or not the individual is formally designated as an officer.

[2] Purchasing is defined, interalia, as the acquisition from a vendor of services, goods or facilities without the transfer of the purchasing firm's non-public proprietary information pertaining to its customers or other information connected with its business activities.

[3] Direct contractual relationships between a third party and a client should not fall within the definition of outsourcing. That is, if a financial institution habitually contracts out a function that could not otherwise perform, then it is not referred to as outsourcing.

xxi. ***"Physical access control"*** refers to the ability to physically touch and interact with computers and network devices. Physical access control enables persons to bypass normal operating system controls and install unauthorised snooping equipment.

xxii. ***"Public tender"*** means the public advertisement of the procurement of e-banking systems or services and inviting responses from interested suppliers.

xxiii. ***"Segregation of duties"*** refers to a basic internal control measure where no employee or group of employees must be in a position to both perpetrate and conceal errors or fraud in the normal course of their duties.

xxiv. ***"Spoofing"*** means impersonating a legitimate customer through use of his/her account number, password, personal identification number (PIN) and/or email address.

xxv. ***"Sniffer"*** is a device that is capable of eavesdropping on telecommunications traffic, capturing passwords and data in transit.

xxvi. ***"Systems"*** refers to the institution's web sites.

xxvii. ***"Telephone banking"*** is a service that banks or other financial institutions provide whereby customers can conduct various financial transactions over the telephone, without having to visit a bank branch or automated teller machine.

xxviii. ***"Transaction"*** means a transfer of benefits, resources, obligations, or the provision of services, regardless of whether a price is charged.

3.0 Introduction

Licensed Financial Institutions (LFIs) introduce a wide range of products and services, including electronic banking (e-banking), to enhance their operational efficiency.

Consequently, their risk management framework must provide the requisite measures to manage and mitigate risks related to e-banking.

This prudential standard seeks to ensure that LFIs implement and promote safe and sound e-banking services and activities that protect the interests of depositors and creditors without stifling technological and financial innovation or competition among financial institutions.

For the purpose of this prudential standard, **Electronic Banking** (e-banking) is defined as –

i. The provision of retail and small value banking products and services through electronic channels as well as large value electronic transactions and other wholesale banking services delivered electronically through the internet, telephone or computerised systems. Noteworthy, licensed financial institutions may offer electronic banking services to both retail and corporate customers.

E-banking can be conducted on one of the following levels:

i. Basic information-only websites and electronic media that provide information on products and services offered. Although customers cannot access account information, they can send e-mail inquiries to the licensed financial institutions;
ii. Simple transactional websites and telephone banking access points whereby customers apply for various services; and
iii. Advanced transactional websites and telephone and mobile banking access points whereby customers can transfer funds between their accounts, make bill payments, query account balances and submit instructions to the bank and other transactions.

E-banking is mostly conducted on a domestic basis, however, some banks may facilitate cross-border e-banking with institutions outside the Eastern Caribbean Currency Union (**see Interpretation section for definition of cross-border e-banking**).

Risks facing licensed financial institutions engaged in e-banking include strategic risk, reputational risk, operational risk (including security and legal risks), credit risk, market risk, and country risk[4]. The Board of Directors and officers of LFIs must recognize these risks and ensure that effective and ongoing risk management controls and systems are in place to appropriately manage the risks.

The Central Bank has realised that LFIs have different risk profiles and as such, the level of e-banking may differ depending on the market, operations and scope of the institutions in the various ECCU territories; hence the prudential standard is wide-ranging and forward looking. The Central Bank has also taken into consideration that a "one size fits all" approach to e-banking may not be appropriate and as such, LFIs must apply this prudential standard based on their scope and level of sophistication of e-banking operations and functions.

The provisions and prudential standard are derived from the principles for Electronic Banking outlined by the Basel Committee on Banking Supervision "Risk Management Principles for Electronic Banking (Basel 2003)" and Basel Committee on Banking Supervision "Management and Supervision of Cross-Border Electronic Banking Activities"[5].

4.0 Application

This prudential standard applies to all institutions licensed under the Banking Act (Licensed Financial Institutions). This standard must be read in conjunction with the Technology Risk Management Standard, Outsourcing Standard, Corporate Governance Standard and any other prudential standard issued by the ECCB. Licensed Financial

[4] Associated with cross-border e-banking.
[5] These core principles can be accessed at http://www.bis.org/publ/bcbs98.pdf and http://www.bis.org/publ/bcbs99.pdf, respectively.

Institutions found in violation of this prudential standard are subject to remedial actions specified in Section 75 of the Banking Act.

5.0 Prudential Standard Requirements

5.1 Role of Board of Directors and Senior Management Officers

5.1.1 The Board of Directors and Senior Management Officers are assigned with the responsibility for developing the Licensed Financial Institution's strategic plan. A clear strategic decision must be made as to whether the Board wishes the Licensed Financial Institution to provide e-banking transactional services prior to offering such services. The Board of Directors must ensure that plans to implement or expand e-banking are in line with the business' strategic goals. The appropriate risk analysis and risk mitigation must be performed and implemented before the decision is made to introduce e-banking services. When implemented, the Board and Management should periodically evaluate the effectiveness of the e-banking strategy. In evaluating the effectiveness, the Board should also consider whether appropriate policies and procedures are in effect and whether risks are properly controlled.

5.1.2 It is binding upon the Board of Directors and the Senior Management officers to take steps to ensure that their institutions have reviewed and modified where necessary, their existing risk management policies and processes to manage the risks associated with current or planned e-banking activities. Further, Licensed Financial Institutions must adopt an integrated risk management approach for all e-banking activities. It is critical that the risk management oversight for e-banking activities becomes an integral part of the

banking institution's overall risk management framework. In addition, the risk management policies must include strategies to mitigate new risk or challenges faced by e-banking activities. If applicable, the risk management framework must also include a focus on cross-border e-banking activities which can expose the institution to country risk and non-compliance with laws and regulations in different foreign jurisdictions (for example consumer protection and anti-money laundering laws).

5.1.3 The Board of Directors and officers must ensure that the operational and security controls are adequate and in place. All key aspects of the Licensed Financial Institution's security control process must be reviewed and approved by the Board of Directors and the senior management team. Further, steps must therefore be taken to ensure that the institution's existing risk management framework including appropriate disclosure principles, due diligence, and oversight processes for outsourcing relationships and other third-party dependencies are appropriately evaluated and modified to accommodate e-banking services.

5.1.4 Moreover, the Board of Directors and officers must ensure that the Licensed Financial Institution does not adopt new technologies or enter into e-banking business or outsource e-banking business unless it has the necessary expertise and framework to provide adequate risk management oversight.

5.1.5 The Licensed Financial Institution must ensure that it has the necessary skill and expertise to manage and/or provide oversight on the technical nature and complexity of the institution's e-banking applications. The board and management must ensure that the organisation is equipped with the requisite skills and technical expertise in line with new technological developments.

5.1.6 The Licensed Financial Institution must ensure that it fosters an effective internal control environment for e-banking including the

consideration of whether the internal and external auditors have the expertise to review e-banking activities and the inclusion of e-banking activities within audit plans.

5.1.7 The Board and Senior Management must provide effective oversight of third party vendors in providing e-banking services and support.

5.2 Security Control And Control Processes For E-Banking

5.2.1 The Licensed Financial Institution must ensure that the necessary security control infrastructure is in place to secure e-banking systems and data from both internal and external threats. This must include but not be limited to, instituting appropriate authorisation, logical and physical access controls, and adequate security infrastructure to maintain appropriate boundaries and restrictions on both internal and external user activities. If e-banking services are outsourced, the appropriate assessment must be conducted to ensure the necessary controls are in place.

5.2.2 The Licensed Financial Institution must ensure that a comprehensive security process is implemented, inclusive of policies and procedures which address possible internal and external security threats both in terms of incident prevention and the appropriate response. The processes must include but not be limited to the following:

a) Physical controls to avert unauthorised physical access to the computing environment.
b) Specialised management and staff to oversee the establishment and maintenance of corporate security policies.
c) Logical controls and monitoring processes including controlled access rights and privileges as well as ongoing monitoring of network intrusion attempts to prevent unauthorised internal and external access (including employees, contractors and those with

access rights through outsourced relationships) to e-banking applications and databases.

d) Ongoing review and testing of security measures and controls; this must include installation of appropriate software upgrades, service packs and other required measures in order to keep abreast with new developments in industry security.

5.2.3 The Licensed Financial Institution must identify and mitigate areas where conflicting duties create the opportunity for insiders to commit fraud. Security profiles must be created, maintained and specific authorization privileges assigned to all users of e-banking systems and applications, including all customers, internal institutional users and outsourced service providers. The ability to interact with data through access control procedures must also be designed to support proper segregation of duties. Institutions must ensure that appropriate measures are taken to protect the data integrity of e-banking transactions, records, and information.

5.2.4 Licensed Financial Institutions must reinforce information security controls to preserve the confidentiality and integrity of customer data. E-banking data and systems must be classified according to their sensitivity and importance and protected in a legally acceptable format. All e-banking transactions must generate clear audit trails, which must be archived and kept for a minimum of five years[6]. Appropriate mechanisms, such as encryption, firewalls to prevent a direct connection of the institution's back end systems and the internet, access control and data recovery plans must be used to protect all sensitive and high-risk e-banking systems.

5.2.5 Storage of sensitive or high-risk data on the organisation's desktop and laptop systems should not be allowed. All sensitive or high-risk data should be stored on the organisation's server and access to such

[6] See ECCB's Anti-Money Laundering Guidance Notes for Licensed Financial Institutions at http://www.eccb-centralbank.org/PDF/Anti-Money.pdf.

information should be granted on a needs basis. Organisations must have recovery plans in keeping with industry best practices related to information technology (IT).

5.2.6 Sufficient physical controls must be in place to deter unauthorised access to all critical e-banking systems. Licensed Financial Institutions must establish fraud detection controls that could prompt additional investigation of suspicious activity.

5.2.7 Licensed Financial Institutions must implement formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-banking services. The incident response and management procedures must allow the institution to identify the origin of the threat speedily, control the damage and assess the magnitude and impact of the incident. Institutions must also identify and notify affected customers. In addition, evidence must be collected and preserved appropriately to facilitate the subsequent investigation and potential prosecution of suspects and intruders. Moreover, the incident response procedures must include strategies for dealing with adverse media and customer reactions in a timely way. Incidents which are deemed significant, and may compromise the operations of the Licensed Financial Institution /or pose a threat to financial stability, should be reported to the Central Bank.

5.2.8 Appropriate systems must be employed to reduce external threats to e-banking systems, including the use of:

a) Adherence to IT policies and procedures including usage of virus-scanning software at all critical entry points (for example remote access servers, e-mail proxy servers).

b) Intrusion detection software and other security assessment tools to sporadically review networks, servers and firewalls for weaknesses and/or violations of security policies and controls.

c) Penetration testing of internal and external networks.

d) A rigorous security review process must be applied to all employees and service providers holding sensitive positions.

5.3 Mobile Online Services

5.3.1 Mobile online services refer to the provision of financial services via mobile devices such as mobile phones or tablets. Customers may choose to access financial services via web browsers on mobile phones or self-developed applications on mobile platforms.

5.3.2 Licensed Financial Institutions that offer mobile online services shall ensure to include in its risk management, controls that address security, authentication and compliance issues. Strategic, transaction, reputation and compliance risks must be covered in the institutions risk management profile.

5.4 Outsourcing

5.3.1 A comprehensive strategy for managing risks associated with outsourcing and third parties in the delivery of e-banking services is mandatory. The strategy must include activities of third party service providers and vendors, including the sub-contracting of outsourced activities that may have a material impact on LFIs.

5.4.2 The institution must ensure that the outsourcing arrangement with the e-banking provider allows for the efficient and timely flow of information and data to the Central Bank, including directly from the third-party service provider, to assist with effective monitoring. The arrangement must allow for examination by the Central Bank, if required.

5.4.3 In accordance with Section 53 (7) of the Banking Act, 2015, prior approval from the Central Bank must be sort by the institution to enter into contractual agreement when an e-banking service is being

outsourced. Additionally, the institution should also inform the Central Bank of any material developments to vary, renew, extend or terminate after entering into the agreement.

5.4.4 To ensure transparency, Licensed Financial Institutions must adopt appropriate procedures for making decisions regarding the outsourcing of e-banking systems or services. The procurement process must be transparent and include the selection of the e-banking service provider via a public tender, where applicable. The selection criteria should be clearly defined and the transactions should be executed using the arm's length principle.

a) It is the responsibility of the Board to ensure that officers conduct a cost-benefit analysis when entering into outsourcing arrangements for e-banking with vendors or third parties.
b) The decision to outsource an e-banking function or service must be consistent with the Licensed Financial Institution's strategic plan. It must also be based on a clearly defined business function, and the specific risks that outsourcing entails must be taken into consideration and mitigating factors implemented.
c) Departments engaged in IT and other staff involved in the e-banking function must have the required knowledge and skills for their respective roles, and understand how the service provider(s) will support the Licensed Financial Institution's e-banking strategy and fit into its overall operating structure.

5.4.5 Due diligence reviews and risk assessments of the service provider on their financial strength, reputation, expertise, technological compatibility, customer satisfaction, risk management policies and controls, and ability to fulfill obligations must be conducted by Licensed Financial Institutions before the selection of e-banking service providers. Thereafter, due diligence and risk assessment must be continued at regular intervals (at least annually) and sometimes on a random basis, to ensure that the service provider is fulfilling its contractual obligations.

5.4.6 Licensed Financial Institutions must ensure that adequate resources are employed to oversee outsourcing arrangements which support e-banking. A committee must be assigned with the responsibility of overseeing e-banking functions and developing an exit strategy for Licensed Financial Institutions to terminate the outsourcing relationship when necessary. A senior member from the IT Department must be placed on the oversight committee. The Licensed Financial Institution's Legal Counsel must examine the exit strategy for any loopholes which may be present in the document.

5.4.7 Licensed Financial Institutions must have a formal contract with the third party service provider that clearly addresses the duties and responsibilities of the parties involved. The Licensed Financial Institutions must implement procedures for ensuring the adequacy of these contracts governing e-banking. The contracts should have specific provisions protecting the privacy and security of the institutions' data, ownership of the data, the right to audit security and controls, the ability of the institution to monitor the quality of service provided, limit the institutions' potential liability for acts of the service provider and termination of contract. These procedures must also include a review by the institution's Legal Counsel and Senior IT officials. Contracts governing outsourced e-banking activities must include the following:

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

b) Execution of a Service Level Agreement detailing the responsibilities and timelines for providing and/or receiving information from the service provider. In order for the Licensed Financial Institutions to sufficiently assess service levels and risks, information from the service provider must be timely and comprehensive. Materiality thresholds and procedures for notifying the Licensed Financial Institution of service

disruptions, security breaches and other events which represent a material risk to the Licensed Financial Institution must be clearly outlined. Materiality thresholds must be included and alluded to in the Licensed Financial Institution's strategic policy, including reporting to the Central Bank.

c) Clauses related to insurance coverage, the ownership of the data stored on the service provider's servers or databases, and the Licensed Financial Institution's right to recover its data if the contract expires or is terminated, must be clearly stated.

d) Clauses to ensure that the service provider complies with the Licensed Financial Institution's policies including performance deliverables, service quality, security controls, financial condition and contract compliance, both under normal and emergency circumstances.

e) Provisions for timely and organised intervention and rectification in the event of poor quality performance or service by the service provider.

f) For cross-border outsourcing arrangements for e-banking, applicable country laws and regulations, including those relating to privacy and other customer protections, must be clearly outlined.

g) The Licensed Financial Institution's right to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans must be unambiguously stated.

h) Independent internal and external audits of outsourced operations must be conducted on a regular basis (at least annually) and must be of the same scope afforded to in-house operations.

i) Licensed Financial Institutions must implement scheduled arrangements for other reviews to be undertaken by independent third parties with sufficient technical expertise, for outsourced

relationships involving critical or technologically complex e-banking services/applications.

5.4.8 Licensed Financial Institutions must ensure that contingency plans are in place for outsourced e-banking activities. The following must be included and implemented as part of the plans:

a) Contingency plans for all critical e-banking systems and services that have been outsourced to third parties must be periodically tested. In addition, contingency plans must be continually developed and kept up to date with technological advancements. In this regard, contingency plans should be reviewed and tested at least annually to ensure relevance to current market conditions.

b) Licensed Financial Institutions must ensure that contingency plans address continuity of e-banking services in the event of natural disasters, other disasters and other worst-case scenarios which could lead to a disruption in outsourced operations.

c) An identified team as well as a standby team must be assigned and made responsible for managing the recovery and assessing the financial impact of a disruption in outsourced e-banking services.

d) The outsourced service provider must provide the Licensed Financial Institution with periodic reports of its internal contingency plan and system recovery testing.

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

5.4.10 It is the responsibility of the Licensed Financial Institution to give service providers the information necessary to identify, control and

monitor any risks associated with the e-banking service arrangement.

5.5 Customer Verification and Authentication

5.5.1 Licensed Financial Institutions must update the customer's profile when their personal information has changed in keeping with anti-money laundering '*Know Your Customer*' procedures. This requirement seeks to reduce the risk of identity theft and fraudulent account applications, promote non-repudiation[7] and establish accountability for e-banking transactions.

5.5.2 Licensed Financial Institutions must implement a multifactor authentication to validate the identity and authorisation of its new and existing customers seeking to conduct electronic transactions.

5.5.3 It is the responsibility of Board of Directors and Officers to ensure that the multifactor authentication is based on management's assessment of the risk posed by the e-banking system as a whole or by the various subcomponents. The risk analysis must assess the transactional capabilities of the e-banking system (for example funds transfer, bill payment, loan origination, account aggregation etcetera.), the sensitivity of the stored e-banking data, and the customer's ease of using the multifactor authentication method.

5.5.4 Officers must implement measures so that the institution can monitor and adopt industry best practices to ensure that:

a) Authentication databases which provide access to e-banking customer accounts or other sensitive systems are secured from

[7] Non-repudiation mitigates the risk of transaction repudiation by creating proof of the origin or delivery of electronic information so as to protect senders from the recipient's false denial of receiving the data or protection of recipients against the sender's false denial of sending the data.

interference and exploitation. Any such interference must be detectable and audit trails must be in place to document such attempts.

b) Any addition, deletion or change of an individual, agent or system to an authentication database is duly authorised by an authenticated source.

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

d) Authenticated e-banking sessions remain secure throughout the full duration of the session and in the event of a timeout, the session must require the user's re-authentication.

e) Data related to financial transactions should not be altered, unless duly authorised and procedures should be in place to ensure that any alteration can be detected.

5.6 Segregation of Duties

5.6.1 Proper controls to ensure segregation of duties would help to reduce the risk of fraud and ensure that transactions are appropriately authorised, recorded and safeguarded. The Licensed Financial Institution must ensure that duties are adequately separated for staff/parties involved in the provision of internal and/or outsourced e-banking services. Segregation of e-banking duties is important in minimizing the opportunity for employee fraud. Controls required to maintain segregation of duties including appropriate authorisation and access privileges need to be adapted, documented and continually reviewed to ensure an adequate level of control is maintained.

5.6.2 The following practices must be used to establish and maintain segregation of duties within an e-banking environment:

a) Transaction processes and systems must be designed to ensure that no single employee or outsourced service provider could originate, authorise and complete a transaction. The LFI's management must identify and mitigate areas where conflicting duties may create the opportunity for insiders to commit fraud.
b) Segregation must be maintained between those initiating static data[8] (including web page content) and those responsible for verifying its integrity.
c) E-banking systems must be tested to ensure that segregation of duties cannot be bypassed.
d) Segregation must be maintained between those developing and those administrating e-banking systems.
e) Ideally, segregation of the responsibilities of the IT security officer / group which deals with information systems security from the IT division, which implements the Licensed Financial Institution's computer systems.
f) Where item (e) is not feasible, specific authorisation/access levels for the IT security officer / group which deals with information systems security from the IT division, which implements the Licensed Financial Institution's computer systems.
g) Specific authorisation must be assigned to all individuals, agents or systems, which conduct e-banking activities. The assigned access privileges should be maintained in an e-banking authorization database.

[8] Static data refers to elements of the internet or computer programming that are fixed or non-changing. A web site that is static can only supply information that is written into the Hyper Text Markup Language (HTML) and this information will not be altered unless the change is written on the source code.

h) All e-banking systems must be fashioned to ensure that they interact with a valid authorisation database.

i) No individual agent or system must have the authority to change his or her own authority or access privileges in an e-banking authorisation database.

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

5.6.3 The Licensed Financial Institution must ensure that appropriate measures are in place to make e-banking authorisation databases reasonably resistant to tampering. Any such tampering must be detectable through ongoing monitoring processes. Sufficient audit trails must exist to document any such tampering.

5.6.4 The Licensed Financial Institution must have a process in place to ensure that any e-banking authorisation database that was tampered with was not used until it was considered secure once more.

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

5.7 Data Integrity of E-Banking Transactions, Records and Information

5.7.1 The following practices must be used by Licensed Financial Institutions to maintain data integrity within an e-banking environment:

a) E-banking records must be stored, accessed and modified in a manner that makes them highly resistant to tampering. If

tampering occurs, it must be detected by transaction processing, monitoring and record keeping functions.

b) E-banking transactions and record-keeping processes must be designed in such a way that it is impossible to avoid detection of unauthorised changes. Moreover, e-banking transactions must be conducted in a manner that makes them highly resistant to tampering throughout the entire process.

c) Licensed Financial Institutions must implement adequate change control policies including monitoring and testing procedures to protect against any e-banking system changes that may erroneously or unintentionally compromise controls or data reliability.

d) External devices including automated teller machines (ATMs), personal computers at remote branches and kiosks that are permanently linked to the institution's network and pass through the firewall must at a minimum address issues relating to non-repudiation, data integrity and confidentiality.

5.8 Audit Trails for E-Banking Transactions

5.8.1 An appropriate independent audit function and the audit program should include the following:

(a) Scope and coverage including the entire e-banking process as applicable, i.e. network configuration and security, regulatory compliance, internal controls and support activities performed by a third party provider;

(b) Personnel with sufficient expertise to evaluate security threats and controls in an open network, i.e. the internet; and

(c) Independent individuals or companies to conduct audits without conflicting e-banking or network security roles.

5.8.2 Licensed Financial Institutions must ensure that clear audit trails are maintained and internal controls independently audited for all critical e-banking events and applications.

5.8.3 Licensed Financial Institutions must adopt the following sound audit practices for e-banking systems:

a) E-banking systems must be designed and installed to capture and hold forensic evidence in a manner where control is maintained over the evidence. In addition, the system must prevent tampering and the collection of false evidence.

b) Logs must be kept for all e-banking transactions for a minimum period of five years to assist in dispute resolution. The log should include at least the user name, receiver information, IP address, date and time of the transaction and transaction amount.

c) Where a third-party service provider assumes the responsibility of processing systems, the Licensed Financial Institution must ensure that the relevant audit trails are kept by the service provider and that the Licensed Financial Institution has access to relevant audit trails, when required. The access must not be predicated on the prior notification by the Licensed Financial Institution.

d) Audit trails maintained by the service provider must meet the Licensed Financial Institution's standards.

5.9 Confidentiality and Privacy of E-Banking Information

5.9.1 Only authorised authenticated individuals, agents or systems must have access to confidential data and records.

5.9.2 All confidential data are maintained securely and protected from unauthorised viewing or modification during transmission over public, private or internal networks.

5.9.3 The institution’s standards and controls for data use and protection must be complied with, when third parties access data through outsourcing relationships.

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

5.9.5 The Licensed Financial Institution must ensure that sufficient information is provided on the institution's websites to allow customer to make informed choices about the identity and regulatory status of the institution, before e-banking transactions are performed. The following must be included on a Licensed Financial Institution's website:

a) The name of the institution and the location of its head office and branches.
b) The profile of the institution Board of Directors and officers.
c) The regulatory authority for the institution (Central Bank).
d) Information for products and services provided by the institution, including interest rates, and fees and charges, etcetera.
e) Contact information for the institution, customer service center regarding products, services, service problems, complaints, suspected misuse of accounts, etcetera.

5.9.6 Licensed Financial Institutions must implement measures to ensure adherence to customer privacy requirements, the following must form part of privacy procedures:

a) All employees, directors and stakeholders would be required to adhere to the institution's established code of conduct which at a minimum must address inter alia, the improper use of confidential information, conflicts of interest, protection and use of the institution's assets and corruption.
b) The Licensed Financial Institution's customer privacy policies and standards take account of and comply with the Banking Act.
c) Customers are informed of the Licensed Financial Institution's privacy policies and relevant privacy issues concerning use of e-banking products and services.
d) Customer data are not used for purposes other than which they are specifically permitted to or for purposes beyond which customers

have authorised or that is mandated by the Central Bank or other legal proceedings.

e) Licensed Financial Institutions must employ appropriate cryptographic techniques, specific protocols or other security controls to ensure the confidentiality of customer e-banking data.

f) Appropriate procedures and controls must be used to periodically assess its customer security infrastructure and protocols for e-banking.

g) Licensed Financial Institutions must ensure that its third-party service providers have confidentiality and privacy policies that are consistent with their own.

h) Licensed Financial Institutions must take appropriate steps to inform e-banking customers about the confidentiality and privacy of their information. These steps may include:

   i. Informing customers of the Licensed Financial Institution's privacy policy.

   ii. Instructing customers of the need to create strong passwords (for example using special characters), protect their passwords, personal identification numbers (PINs) and other banking and/or personal data.

   iii. Informing customers of the institution's requirement to implement expiry timelines for use of passwords).

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

5.10 E-Banking Business Continuity and Contingency Planning

5.10.1 To help ensure continuity of e-banking services, Licensed Financial Institutions must have in place appropriate business continuity and

contingency plans. E-banking services and applications, including those provided by third-party service providers, must be identified and assessed for criticality.

5.10.2 Risk assessments for each critical e-banking service and application, including the potential implications of any business disruption on the Licensed Financial Institution's legal and reputation risk must be conducted prior to the launch of the product.

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

5.10.4 Defined thresholds or capacity limits to indicate the maximum number of customers/transactions that can be accommodated by the institution’s e-banking services must be established. The institution must also develop processing alternatives for managing demand when e-banking systems appear to be reaching the defined capacity levels.

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

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

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

services, thus the current and future capacity of critical e-banking delivery systems must be assessed on an ongoing basis.

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

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

5.11 E-Banking Incident Response Plans

5.11.1 Licensed Financial Institutions must develop appropriate incident response plans, including communication strategies that ensure business continuity, minimise operational, legal and reputational risks and limit liability associated with disruptions in their e-banking services including those originating from outsourced systems and operations.

5.11.2 To ensure effective response to unforeseen incidents, Licensed Financial Institution must develop:

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

b) Mechanisms to identify an incident or crisis as soon as it occurs, assess its materiality, and control the reputation risk associated with any service disruption.

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

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

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

f) A clear chain of command, encompassing both internal as well as outsourced operations, to ensure that prompt action is taken appropriate for the significance of the incident. In addition, escalation and internal communication procedures must be developed and include notification of the Board and Senior management on the probable damage and potential monetary loss associated with the incident.

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

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

6.0 Regulatory Reporting Requirements

6.1 Each Licensed Financial Institution shall submit a copy of their e-banking strategic plan and outsourcing strategy to the Central Bank within 30 days of approval by the Board. Any revisions to the strategic plan shall be submitted to the Central Bank, as they are approved.

6.2 Licensed Financial Institutions shall submit to the Central Bank all outsourcing agreements for approval.

6.3 The institutions' risk management policy shall be submitted to the Central Bank within 30 days of approval by the Board.

6.4 Security process implemented by the institution shall be submitted to the Central Bank. Additionally, all incident reports and response shall be sent to the Central Bank within 3 days of the occurrence. Any further update on the incident shall also be reported to the Central Bank.