CENTRAL BANK OF SEYCHELLES

P. O. Box 701, Victoria, Seychelles

Telephone: [+248] 428 20 00
Fax: [+248] 432 36 65
E-mail: enquiries@cbs.sc

Ref: FSD/GEN/1

Date: April 09, 2019

To all deposit-taking financial institutions such as banks and credit unions

Cyber security guidelines for deposit-taking financial institutions

The Central Bank of Seychelles (CBS) hereby issues these guidelines on cyber security to deposit-taking financial institutions such as banks and credit unions with the aim of promoting and enhancing cyber-risk management practices in the financial sector. Such financial institutions should adopt these guidelines while establishing a cyber-defense array in accordance with the scope and the nature of its business activity and risk profile.

CBS trusts in your cooperation.

C. Abel (Ms)
Governor

Central Bank of Seychelles
Cyber Security Guidelines
2019

Table of Contents

1. Introduction **2**

2. Structure of the Guidelines **4**

2.1. Cyber Security Policy and Governance 4

2.2. Cyber-risk assessment 5

2.3. Independent Security Assessment 6

2.4. Incident Response and Crisis Management Plan 6

2.5. Continuous Monitoring of financial institutions' environment 8

2.6. Cyber Security Awareness Programme 8

2.7. Supply Chain Management 9

2.8. Reporting to Central Bank of Seychelles 10

2.9. Other General Technical Control 10

2.9.1. Management of Business Information Assets 10

2.9.2. Network Management and Security 10

2.9.3. User Access Management 11

2.9.4. Secure Configuration 11

2.9.5. Patch/Vulnerability and Change Management 11

2.9.6. Authentication mechanism for Customers 12

2.9.7. Secure mail and messaging systems 12

2.9.8. Removable Media 12

2.9.9. Threat Monitoring 12

2.9.10. Anti-Phishing 13

2.9.11. Data Loss prevention 13

2.9.12. Metrics 13

Appendix A. - Glossary **14-15**

Appendix B. - Template for reporting Cyber Security Incidents and Root Cause Analysis **16-18**

1. Introduction

The advancement of information technology has fundamentally changed business processes and models in financial institutions of all sizes. These advancements have introduced efficiencies and cost savings for financial institutions and their customers. At the same time, these technologies may also bring significant risks as financial institutions become increasingly interconnected and more reliant on complex IT systems and outsourcing service providers to conduct their business and deliver services to customers. In addition, whilst the adoption of technological innovations has reduced costs and increased efficiencies, it has concurrently provided greater risks for data to be lost, stolen, corrupted or accessed by unauthorised users. Cyber criminals are also constantly finding new ways to attack, breach, and exploit financial institutions. Financial institutions are prime targets and need to pro-actively create, fine-tune their policies, procedures and technologies based on new developments and emerging concerns.

The Central Bank of Seychelles (CBS) is cognisant that cyber-risk will keep morphing due to the evolution of cyber threats across the globe. Therefore, these Cyber Security Guidelines (the ''Guidelines'') have been issued to promote a structured but flexible framework for cyber-risk management, while allowing the financial institution to exercise discretion in its implementation. This approach is intended to enable the financial institution to adapt its defence system in a dynamic manner to the changing cyber threat landscape. It emphasises that the board and senior management of financial institutions should view cyber-risk as a corporate-wide concern which requires the active involvement of senior officials of financial institutions.

Application

The Guidelines are intended to apply to deposit-taking financial institutions such as banks and credit unions (collectively referred to as ''financial institutions'').

Purpose

The Guidelines outline the minimum requirements that financial institutions should build upon in the development and implementation of cyber strategies, policies, procedures and related activities aimed at mitigating cyber-risks. Therefore, the purpose behind the Guidelines is to:

- Create a safer and more secure cyberspace that underpins information system security priorities and promote the stability of the financial sector
- Establish a coordinated approach to the prevention and response to cyber crime
- Promote compliance with appropriate technical and operational cyber security standards
- Develop requisite skills, continuous building of capacity and promote a culture of fostering a strong interplay between policy, leveraging on technology to do business and risk management and
- Maintain public trust and confidence in the financial system.

The Guidelines are not a replacement for and does not supersede the legislation, regulations and other requirements that financial institutions must comply with as part of their regulatory obligations, particularly in the areas of risk management, outsourcing, information communication technology, internal controls and corporate governance.

Responsibility

It is the responsibility of the board of directors and senior management of financial institutions to set minimum standards to protect information assets. Concurrently, the expectation is that financial institutions should adopt the Guidelines while establishing a cyber-defence array in accordance with the scope and the nature of its business activity and risk profile.

It is important to note that the Guidelines do not address all aspects of the management of cyber security risk but rather focus on those areas that are deemed most pertinent at this point in time. It is the responsibility of the management of the financial institution to understand the specific cyber related risks that the institution faces and to ensure that these are sufficiently mitigated in line with their risk appetite. It is acknowledged that the relevance and importance of the issues raised in the Guidelines will vary according to the business model, size and technological complexity of the institution and the sensitivity and value of its information and data assets.

2. Structure of the Guidelines

2.1. Cyber Security Policy and Governance

Establishing, maintaining and monitoring an information security governance framework enables financial institutions to set clear direction for, and demonstrate their commitment to information security.

- Financial institutions should review these arrangements so that security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable prompt action
- Financial institutions should create the control and necessary reporting mechanisms for managing cyber security risk effectively.

A comprehensive, documented cyber security policy provides the commitment to cyber security in order to address the need for the entire financial institution to contribute to a cyber safe environment. The cyber security policy should be distinct and separate from the broader Information Technology policy so that it can highlight the risks from cyber threats and measures to mitigate these risks.

- Financial institutions should put in place a cyber security policy elucidating the strategy and containing an appropriate approach to combat cyber threats
- The policy should be duly approved by the board and communicated to staff and third parties. The cyber security policy shall cover secure and acceptable use of the financial institution's network and assets, including the handling of customer information and educating staff about the risks and protection measures at their level
- Financial institutions should review their cyber security arrangements, policies and supporting framework based on each financial institution's threat and vulnerability assessments on a yearly basis or when there is significant change(s).

The policy should be supported with relevant standards, guidelines and procedures. At a minimum, the policy should incorporate and take into consideration the following:

- Objectives, scope, ownership and responsibility for the policy
- Information security roles and responsibilities that may include information security-specific roles such as IT security manager/officer, administrators, information security specialists and information asset-specific roles e.g. owners, custodians, end-users etc.
- Periodic reviews of the policy at least annually and in the event of significant changes necessitating revision
- A periodic compliance review of the policy about the adherence of users to information security policies and put up to the information security committee
- Measures for violation of policies and the process to be followed in the event of violation
- Identification, authorisation and granting of access to IT assets (by individuals and other IT assets)

- Addressing the various stages of an IT asset's life cycle to ensure that information security requirements are considered at each stage of the lifecycle
- An incident monitoring and management process to address the identification and classification of incidents, reporting, escalation, preservation of evidence and the investigation process
- Management of technology solutions for information security e.g. firewalls, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques
- Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers)
- Strategy for periodic training and enhancing skills of information security personnel including requirements for continuous professional education.

Financial institutions should have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting to the board and senior management and customer communication, where appropriate.

Financial institutions should provide key decision-makers, senior management and the board of directors with an informed view of:

- Aspects of effectiveness and efficiency of information security monitoring arrangements
- Areas where improvement is required
- Information and systems that are subject to an unacceptable level of risk
- Performance against quantitative and objective targets and
- Actions required to help minimise risk (e.g. reviewing the risk appetite, understanding the information security threat environment and encouraging business and system owners to remedy unacceptable risks).

2.2. Cyber-risk assessment

The size, technological complexity, digital products and threat perception varies between financial institutions and hence it is important to identify the inherent risks and controls on a regular basis. While identifying and assessing the inherent risks, it is important to take into consideration the technologies adopted, alignment with business and regulatory requirements, connections established, delivery channels, online including mobile products, technology services, organisational culture as well as internal and external threats.

This principle details the requirements of an effective process for cyber-risk identification and assessment:

- Taking into account the dynamic nature of the cyber domain, financial institutions are expected to carry out an ongoing examination of cyber-risks. They should identify and assess the cyber threats and risks and measure the effectiveness of their respective mitigating controls

- Reports on the current status of cyber-risks should be delivered to senior management and the board of directors on a regular basis to provide them with an accurate, comprehensive and coherent view of cyber-risks across the financial institution.

In broad terms, the risk management process consists of:

- Identification of assets and estimation of their value. Aspects to be included are people, buildings, hardware, software, data and supplies
- Conducting a threat assessment, which may include aspects such as acts of nature, acts of war, accidents and malicious acts originating from inside or outside the financial institution
- Calculating the impact that each threat would have on each asset through qualitative or quantitative analysis
- Identifying, selecting and implementing appropriate controls including considerations such as productivity, cost effectiveness and the value of the asset
- Evaluating the effectiveness of the control measures and ensuring the controls provide the required cost-effective protection.

2.3. Independent Security Assessment

The cyber security status of target environments (e.g. critical business environments, processes, applications and supporting systems/networks) should be subject to independent and regular security audits to ensure that security controls have been implemented effectively and cyber-risks are being adequately managed.

- Financial institutions should conduct thorough, independent and regular security audits and provide the owners of target environments and senior management with an independent assessment of their security status
- Financial institutions should periodically conduct network security review, vulnerability assessment and penetration testing exercises for all critical systems, particularly those exposed to the internet. Penetration testing of public facing systems as well as other critical applications should be carried out by professionally qualified teams
- The vulnerabilities detected should be remedied promptly as part of the financial institution's risk management framework to avoid exploitation of such vulnerabilities
- Findings of vulnerability assessments and penetration testing and the follow-up actions necessitated should be monitored closely by senior management.

2.4. Incident Response and Crisis Management Plan

Financial institutions are expected to be well prepared to face emerging cyber threats such as 'zero-day' attacks, remote access threats and targeted attacks. Financial institutions should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to distributed denial of services (DDoS) attacks, ransomware, email spam, phishing and identity fraud etc.

Financial institutions should be able to manage a major crisis by having an incident management capability and establishing a crisis management team.

- Financial institutions should put in place a fully effective incident response plan to respond to and document information security incidents with due approval of the board and senior management. This incident response plan should include the roles of its staff as well as staff of outsourcing service providers when handling such incidents

- Financial institutions should define incidents, method of detection, methods of reporting incidents by staff, vendors and customers as well as the expected response in each scenario and incident type in the incident response plan

- Financial institutions should also allocate and communicate clear roles and responsibilities to staff handling such incidents and provide specialised training to such staff, conduct post incident reviews and periodically test their incident response plans

- Financial institutions should ensure such capabilities in all interconnected systems, networks including those of vendors and partners and readiness demonstrated through collaborative and coordinated resilience testing that meet their recovery time objectives

- Financial institutions should promptly incorporate lessons learnt to continually improve their response strategies

- Major activities that should be considered as part of the incident management framework include:

    a) Developing and implementing processes for preventing, detecting, analysing and responding to information security incidents
    b) Establishing escalation and communication processes and lines of authority
    c) Establishing the capability to investigate information security incidents through various modes such as forensics, evidence collection and preservation, log analysis etc.
    d) Developing a process to communicate with internal parties and external organisations (e.g. regulator, media, law enforcement, customers)
    e) Organising, training and equipping staff to effectively respond to information security incidents
    f) Periodically testing and refining the incident response plan
    g) Conducting post-mortem analysis and reviews to identify causes of information security incidents, develop corrective actions and reassess risk, and adjust controls suitably to reduce related risks in the future
    h) Integrating the incident response plan with the financial institutions' disaster recovery (DR) and business continuity plan (BCP)

- Financial institutions' BCP and DR capabilities should adequately and effectively support their cyber resilience objectives. This should be designed to enable the financial institution to recover rapidly from cyber-attacks and other incidents as well as be able to safely resume critical operations aligned with recovery time objectives whilst ensuring security of information

- A crisis management plan should be established and supported by a crisis management team, which details actions to be taken in the event of a major incident or serious cyber-attack to

respond quickly and effectively reducing any potential business impact including brand and reputational damage

- Financial institutions should take effective measures to prevent cyber-attacks and promptly detect any cyber-intrusions to respond, recover and contain any incident
- The crisis management plan should address the following four aspects:
    a) Detection
    b) Response
    c) Recovery
    d) Containment.

2.5. Continuous Monitoring of financial institutions' environment

It is important for financial institutions to continuously monitor critical infrastructure and keep abreast with the latest nature of emerging cyber threats.

- Financial institutions should implement and periodically validate settings for capturing appropriate logs and audit trails of each device, system software and application software. The financial institution should ensure that logs include minimum information to uniquely identify the log e.g. by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction
- Financial institutions should manage and analyse audit logs in a systematic manner to detect, understand or recover from an attack. The integrity of the logs should be maintained to support forensic investigations if needed
- A security event management process may be established to identify, investigate, and help respond to security-related events in a timely manner
- Threat intelligence may be created based on analysis of a range of sources, which is relevant, insightful, contextual and actionable.

2.6. Cyber Security Awareness Programme

It is important for financial institutions to provide ongoing training and cyber security awareness programmes. This should provide information on good security practices, common threat types and the financial institution's policies and procedures. Training should be provided to all staff including senior management as well as the board as managing cyber-risk requires the commitment of the entire financial institution to create a cyber-safe environment.

- The cyber security awareness programme should be mandatory for all staff and should be conducted at least annually
- The financial institution should periodically evaluate the level of cyber security awareness of staff

- Financial institutions should conduct targeted awareness programmes for key personnel e.g. at executive, operations, security related administration and operation and management roles, to raise awareness on evolving cyber threats
- Board members should be sensitised on various technological developments and cyber security related developments periodically. They may be provided with yearly awareness programmes on cyber security risk and evolving best practices
- Cyber security awareness should be provided to the financial institution's customers, suppliers, outsourcing service providers and other third parties who have links to the financial institution's IT infrastructure
- Financial institutions should improve and maintain customer awareness and education with regard to cyber security risks. They should be educated on the downside risk of sharing their login credentials e.g. passwords to any third party and the consequences thereof. Customers should be encouraged to report on phishing mails and phishing sites so that financial institutions can take effective remedial action.

2.7. Supply Chain Management

- Financial institutions are expanding their reliance on outsourcing and other third-party service providers in a variety of different capacities. These providers may often perform important functions for the financial institution and may require access to confidential information, applications and systems. Financial institutions may be exposed to cyber threats through these third-party service providers. Therefore, it is important that financial institutions ensure that the relevant third parties also implement mechanisms to mitigate their exposure to cyber risks and comply with legal and regulatory frameworks
- Financial institutions should establish appropriate policies and procedures to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor and outsourcing activities
- Financial institutions should have in place adequate governance of outsourcing agreements including due-diligence on prospective third-party service providers and adequate monitoring of service delivery. This may include, but is not limited to non-disclosure agreements, the right to audit and security policy compliance agreements with the third-party service provider
- Financial institutions should adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of information out of borders
- Financial institutions should monitor contracted third parties for changes in their business and cyber posture including expansions, divestitures, breaches and new attacks that may affect the financial institution. Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics or penalties
- Financial institutions should develop exit management strategies and contingency plans for their relevant third party providers.

2.8. Reporting to Central Bank of Seychelles

Financial institutions should notify CBS within 24 hours of any cyber security incident that could have a significant and adverse impact on the financial institution's ability to provide adequate services to its customers, its reputation or financial condition in the format set out in Appendix B of the Guidelines. A root cause analysis (RCA) of the cyber security incident should also be conducted and the report provided to CBS within 14 days following the detection of the cyber security incident as per the format in Appendix B.

2.9. Other General Technical Control

The list below provides a set of general technical control that should be put in place by financial institutions to achieve baseline cyber security resilience. This should be evaluated periodically to integrate risks that arise due to evolving security threats.

2.9.1. Management of Business Information Assets

- Maintain an up-to-date inventory of assets, including business information, customer information, business applications, supporting IT infrastructure and facilities e.g. hardware/software/network devices, key personnel, services, etc. indicating their business criticality. The financial institution may have their own framework and criteria for identifying and classifying critical assets
- Secure the way information is stored, transmitted, processed, accessed and used within and outside the financial institution's network and manage the level of risk they are exposed to depending on the sensitivity of the information.

2.9.2. Network Management and Security

- Prepare and maintain an up-to-date network architecture diagram at the institution level including wired and wireless networks
- Maintain an up-to-date and centralised inventory of authorised devices connected to the financial institution's network (within and outside financial institution's premises). Financial institutions should implement solutions to automate network discovery and management to automatically identify unauthorised device connections to the network and block such connections
- Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security
- Put in place appropriate controls to secure wireless local area networks (LAN), wireless access points and wireless client access systems
- Financial institutions should have mechanisms to identify authorised hardware and mobile devices such as laptops, mobile phones, tablets etc. and ensure that they are only provided connectivity if and only if, this is necessary and subject to the policies and security requirements of the financial institution
- Implement mechanisms to detect and remedy any unusual activities in systems, servers, network devices and endpoints
- Boundary defences should be multi-layered to filter both inbound and outbound traffic.

2.9.3. User Access Management

- Provide secure access to the financial institution's assets and services from within and outside the network by protecting information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. by using Virtual Private Networks (VPN) or other secure web protocols)
- Carefully protect customer access credentials such as log on User ID, authentication information and tokens, access profiles against cyber-attacks
- Disallow administrative rights on end-user workstations (PCs and/or laptops) and provide access rights on a need to know basis for specific purpose and duration when it is required following an established process
- Implement centralised authentication and authorisation system for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties
- Implement appropriate systems and controls to allow, manage, log and monitor privileged administrative access to critical systems (e.g. servers/operating system/database, applications, network devices etc.)
- Implement controls to minimise invalid log on counts and deactivate dormant accounts
- Monitor any abnormal change in log on patterns
- Implement measures to control use of macros in documents as well as permissible attachment types in emails.

2.9.4. Secure Configuration

- Apply baseline security configurations to all categories of devices (endpoints, operating systems, databases, applications, network devices, security devices, security systems etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically
- Periodically evaluate critical device (e.g. firewalls, network appliances, security devices, etc.) configurations and patch levels for all systems in the network, third-party hosted sites and shared-infrastructure locations.

2.9.5. Patch/Vulnerability and Change Management

- Document the inventory of IT components that need to be patched
- Identify and apply the necessary patches to minimise the number of vulnerable systems and the window of vulnerability/exposure
- Implement systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of server operating systems/databases/applications, etc.
- Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes and configuration baseline that ensures integrity of any changes thereto
- Periodically conduct vulnerability assessment and/or penetration testing of internet facing web/mobile applications, servers and network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)

- Periodically conduct software security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environments closely resembling to or in a replica of the production environment
- As a threat mitigation strategy, identify the root cause of incidents and apply necessary patches to plug the vulnerabilities
- Periodically evaluate the access device configurations and patch levels to ensure that all access points nodes between:
    a) different Virtual Local Area Networks (VLANs) in the server room;
    b) Local Area Network/Wide Area Network (LAN/WAN) interfaces
    c) The financial institution's network and external networks; and
    d) interconnections with partner, vendor and service provider networks

  are securely configured.

2.9.6. Authentication mechanism for customers

- Implement authentication mechanisms to provide positive identification verification of the financial institution to customers
- Customer identification information should be kept secure
- Financial institutions should act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

2.9.7. Secure mail and messaging systems

- Implement secure mail and messaging systems including measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

2.9.8. Removable Media

- Define and implement a policy for restriction and secure use of removable media, Bring your own device on various types/categories of devices including but not limited to workstations/PCs/laptops/mobile devices/servers, etc. and erasure of data on such media after use
- Financial institutions should limit media types and information that could be transferred or copied to and from such devices
- Removable media should be scanned for malware and viruses prior to provide read/write access
- Consider implementing centralised policies through Active Directory or endpoint management systems to whitelist/blacklist/restrict removable media use
- As a default rule, use of removable devices and media should not be permitted in the financial institution's cyber environment unless specifically authorised for defined and duration of use.

2.9.9. Threat Monitoring

- Implement anti-malware and antivirus protection including behavioral detection systems for all categories of devices (e.g. endpoints such as PCs/laptops/mobile devices), servers (operating systems, databases, applications, etc.), web/internet gateways, email-gateways, wireless

networks, SMS servers etc. including tools and processes for centralised management and monitoring

- Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS etc.) traffic passing through the web/internet gateway
- Consider implementing whitelisting of internet websites/systems.

2.9.10. Anti-Phishing

- Consider subscribing to anti-phishing services from external service providers for identifying and taking down phishing websites.

2.9.11. Data Loss prevention

- Financial institutions should develop a data loss and leakage prevention policy to safeguard sensitive, including confidential, business and customer information. This should include protecting data processed in endpoint devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

2.9.12. Metrics

- Financial institutions should develop a comprehensive set of metrics that provide for prospective and retrospective measures such as key performance indicators and key risk indicators. Illustrative metrics may include coverage of anti-malware software and patch latency, extent of user awareness training and vulnerability related metrics.

Appendix A. - Glossary

- **Business continuity:** The capability of the organisation to continue operations at acceptable predefined levels following a disruptive incident.
- **Cyber-attack**: The use of an exploit by an adversary to take advantage of a weakness with the intent of achieving an adverse effect on the business operations.
- **Cyber-risk**: The combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for an organisation.
- **Cyber security:** Refers to the set of controls and organisational measures and means (human, technical, etc.) used to protect information system assets and communication networks against all non-physical attacks, irrespective of the attack being initiated through a physical or logical security breach. Controls and measures include preventing, detecting and responding to all malicious IT activities perpetrated to information system assets, potentially affecting systems or data confidentiality, integrity or availability, as well as the traceability of operations executed on these information systems and networks.
- **Cyber security risk management**: The process used by an organisation to establish an enterprise-wide framework to manage the likelihood of a cyber-attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber-attack. The management of an organisation's cyber-risk should support the business processes and be integrated into the organisation's overall risk management framework.
- **Endpoint**: Refers to PCs, laptops and mobile devices.
- **Information Asset:** Refers to data, hardware, software, networks or other elements of an organisation's IT landscape that support information-related activities.
- **Outsourcing**: Refers to a financial institution's use of a third party (the "outsourcing service provider") to perform activities that would normally be undertaken by the financial institution, now or in the future.
- **Service provider:** the supplier of goods, services or facilities, which may or may not be a regulated entity, and which may be an affiliated entity within a corporate group or an entity that is external to the group.
- **Risk appetite**: The aggregate level and types of risk an organisation is willing to assume within its risk capacity to achieve its strategic objectives and business plan.
- **Security event**: Any observable occurrence in a system and/or network. Events sometimes provide an indication that an incident is occurring.
- **Security incident:** An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

- **Vulnerability:** A weakness in a system, application, or network that is subject to exploitation or misuse.

Appendix B – Template for reporting cyber security incidents and root cause analysis

Template for reporting cyber security incidents

Basic Information	
1. Particulars of Reporting	
Name of Financial Institution	
Date and Time of Reporting to CBS	
Name of person reporting	
Designation	
Contact details (email, phone number)	
2. Details of Cyber Security Incident	
Date and Time of Incident Detection	
Nature of Cyber Security Incident (e.g. DDOS, ransomware etc.) Affected areas (i) Outage of critical IT systems (e.g. Core banking system, treasury systems, ATMs, internet banking, payment system etc.) (ii) Theft or Loss of Information (e.g. sensitive customer or business information stolen, missing, destroyed or corrupted) (iii) Outage of Infrastructure (e.g. which premises or branch, domain control/central processing units, etc., power/utilities supply, telecommunications supply) (iv) Others (E.g. financial, outsourced service providers etc.)	
3. Impact Assessment (examples are given but are not exhaustive):	
Business impact including on availability of services e.g. banking services, internet banking, cash management, trade finance, branches, ATMs, clearing and settlement activities, etc.	
Impact on stakeholders e.g. affected retail and corporate customers, affected participants including operators, settlement institution, business partners and service providers, etc.	

Financial and market impact e.g. on trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds etc.	
Regulatory and legal impact	
4. Chronological order of events	
Date of incident, start time and duration	
What actions have been taken by the financial institution since detection of the incident? Please include escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measure	
Stakeholders informed or involved	
Channels of communications used (e.g. email, internet, SMS, press release, website, notice etc.)	
Rational on the decision/activation of BCP and/or DR	

Template for Root Cause Analysis Report

5. Root Cause Analysis (RCA)	
Factors that caused the problem/reasons for occurrence	
Interim measures to mitigate/resolve the issue and reasons for taking such measures	
Steps identified or to be taken to address the problem in the longer term. Please list the remedial measures and/or corrective actions taken to prevent future occurrence of similar types of incidents	
Date/Target date of resolution	

Please submit the cyber security incident report within 24 hours after a cyber security incident[1] to the Financial Surveillance Division (FSD) using the email address: fsdreturns@cbs.sc.

[1] As per section 2.8 of the Guidelines, this applies to any cyber security incident that could have a significant and adverse impact on the financial institution's ability to provide adequate services to its customers, its reputation or financial condition and a RCA should be conducted for such cyber security incidents.

The RCA report should be submitted to the FSD using the same email address within 14 days following the detection of the cyber security incident. Financial institutions may also be requested to provide any other additional information.