

# **BANK OF BOTSWANA**

## **PRUDENTIAL AUTHORITY AND PAYMENTS OVERSIGHT DEPARTMENT**



## **GUIDELINES ON CYBERSECURITY AND RESILIENCE**

**Issue Date: May 31, 2023**

## Contents

1.	AUTHORITY, PURPOSE AND SCOPE .....	2
2	INTRODUCTION .....	3
3.	DEFINITION OF TERMINOLOGY .....	4
4.	CYBER RISK MANAGEMENT AND OVERSIGHT .....	9
(a)	GOVERNANCE .....	9
(i)	Cyber-Resilience Strategy .....	9
(ii)	Cyber-Resilience Framework .....	10
(iii)	Board and Senior Management Responsibilities .....	10
5	CYBER-SECURITY FUNDAMENTAL ELEMENTS .....	12
(a)	IDENTIFICATION .....	12
(i)	Asset Management .....	13
(ii)	Risk Assessment .....	13
(b)	PROTECTION .....	14
(i)	Identity and Access Management .....	14
(ii)	Security Awareness and Training .....	14
(iii)	Human Resource Security .....	15
(iv)	Network and Infrastructure Management .....	15
(v)	Systems Acquisition and Development .....	16
(vi)	Change and Patch Management .....	17
(c)	DETECTION .....	18
(i)	Anomalies and Events .....	18
(d)	TESTING .....	19
(i)	Vulnerability Management .....	19
(ii)	Scenario-Based Testing .....	20
(iii)	Penetration Tests .....	20
(iv)	Red-Team Testing .....	20
(e)	RESPONSE AND RECOVERY .....	21
(i)	Cyber-resilience Incident Management .....	21
(ii)	Data Integrity .....	22
(iii)	Communication and Collaboration .....	22
(iv)	Crisis Communication and Responsible Disclosure .....	23
(v)	Supply Chain and Dependency Management .....	23
(vii)	Cyber Threat Intelligence .....	24
(viii)	Information Sharing .....	25
	APPENDIX .....	26
	Appendix A: Cybersecurity Incident Reporting Form .....	26

## **1. AUTHORITY, PURPOSE AND SCOPE**

### **(a) Authority**

- 1.1 These guidelines are issued by the Bank of Botswana (Bank), pursuant to its authority set forth in Section 4C (1) of the Bank of Botswana (Amendment) Act, 2022 (Cap. 55:01).

### **(b) Purpose**

- 1.2 The purpose of these guidelines is to provide guidance for banks to

- (a) enhance their cyber posture and resilience.
- (b) create a common approach for addressing cyber risk within the banking system.
- (c) achieve minimum and acceptable levels of cyber resilience.
- (d) ensure that systemic cyber risk is properly managed within the banking system.
- (e) comply with principle 7 of Principles for Operational Resilience issued by the Basel Committee on Banking Supervision and
- (f) expand the operational risk management guidelines as stated in the 2018 Guidelines on Risk Management to include cyber risk management.

### **(c) Scope of Authority**

- 1.3 These guidelines apply to banks licensed under the Banking Act (Cap. 46:04) (Banking Act), statutory banks and other financial institutions established under separate Acts of Parliament, but falling within the purview of the Bank's supervision in terms of Section 53(2) of the Banking Act. In implementing the guidelines, institutions are expected to use a risk-based approach by evaluating their current environments, identifying gaps and prioritising mitigation of identified high risks. In addition, institutions should take into account the following:

- (a) Process for compliance: financial institutions must send their self-assessment against the guidelines to the Bank within 90 days from the date of issue of the guidelines, and subsequently by December 31 each year.
- (b) Proportionality – all financial institutions should comply with the provisions set out in the guidelines in such a way that is proportionate to, and takes account of, the size, internal organisation, complexity and risk of the financial institution's operations and information and communications technology.
- (c) Incident reports – a financial institution must report, in the form and manner determined by the Bank, any material systems failure, malfunction, delay or other disruptive event or cyber incident, that are classified as material, within 48 hours of occurrence.

(d) Clarification – any questions that arise as to the interpretation and application of the guidelines should be addressed to the Director, Prudential Authority and Payments Oversight Department.

(e) Entry into force – the guidelines come into force on the date of its publication.

## **2 INTRODUCTION**

2.1 Cyber-attacks are increasing in frequency, sophistication and impact, with perpetrators continually refining their efforts to compromise systems, networks and information world-wide. The financial sector is one of the prime targets for such attacks, given the intensive use of technology in the sector.

2.2 Therefore, the Bank of Botswana has developed these cybersecurity and resilience guidelines in order to raise awareness, and promote the governance and management of cyber risk within the sector. The guidelines are based on the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC 27001), Control Objectives for Information and Related Technology (COBIT 5), The National Institute of Standards Cybersecurity Framework (NIST CSF), Information Security Forum's Standard of Good Practice for Information Security (ISF), and international best practices, and seek to set out requirements for financial institutions to improve their cyber-resilience posture.

2.3 The guidelines primarily serve as an overarching framework for the governance and management of cyber risk, which financial institutions can tailor to their own specific needs and technologies, taking into account the principle of proportionality.

2.4 The key components of the guidelines comprise the following:

(a) Governance: cyber governance refers to the arrangements a financial institution has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber-resilience framework that prioritises the security and efficiency of a financial institution's operations and supports financial stability objectives. The framework should be guided by a financial institution's cyber-resilience strategy, define how the financial institution's cyber-resilience objectives are determined, and outline its people, processes and technology requirements for managing cyber risks and timely communication, in order to enable a financial institution to collaborate with relevant stakeholders to effectively respond to and recover from cyber incidents. The framework should be supported by clearly defined roles and responsibilities of the board and senior management of a bank. The board and senior management should cultivate a culture that ensures a high level of accountability by staff at all levels regarding effective cyber resilience.

(b) Identification: given that a financial institution's operational failure can negatively affect financial stability, it is crucial that financial institutions identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. After the identification or asset classification process, the financial institution must have a robust risk assessment process in place to determine the criticality of its assets and how to protect them using a variety of controls.

- (c) **Protection:** a financial institution's ability to implement effective security controls and system process designs that protect the confidentiality, integrity and availability of its assets and services.
- (d) **Detection:** A financial institution's ability to recognise signs of a potential cyber incident or detect breach incidents is essential to strong cyber resilience. Early detection of cyber incidents provides a financial institution with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches.
- (e) **Testing:** testing is an integral component of any cyber-resilience framework. All elements of a cyber-resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within a financial institution and regularly thereafter. Sound testing regimes, such as vulnerability assessments, scenario-based testing, penetration tests and tests using red teams (that is, ethical hackers) can produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the financial institution's cyber-risk management process.
- (f) **Response and recovery:** financial stability may depend on a financial institution's ability to transact in the financial markets, settle obligations on due dates, or discharge critical functions. Therefore, a financial institution's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to perform these critical functions. Business continuity planning is essential in meeting related objectives, and having effective incident response and crisis management protocols is critical.
- (g) **Situational awareness:** refers to an institution's ability to identify, process and comprehend the critical elements of information through a cyber-threat intelligence process that provides a level of understanding that is relevant to act upon in mitigating the impact of a potentially harmful event. Strong situational awareness, acquired through an effective cyber-threat intelligence process and participation in information-sharing arrangements, can make a significant difference in the financial institution's ability to pre-empt cyber events or respond rapidly and effectively to them.

### **3. DEFINITION OF TERMINOLOGY**

- (a) **Access control:** to ensure that access to assets is authorised and restricted, having regard to business and security requirements.
- (b) **Advanced persistent threat (APT):** a threat actor that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple threat vectors. The APT pursues its objectives repeatedly over an extended period of time, adapts to defenders' efforts to resist it, and is determined to execute its objectives.



- (c) Asset: something of either tangible or intangible value that is worth protecting, including personnel, information, infrastructure, finance and reputation.
- (d) Authenticity: a property that an entity is what it claims to be.
- (e) Availability: property of being accessible and usable on demand by an authorised entity.
- (f) Blue team: a team that evaluates organisational security environments and defends these environments from red teams.
- (g) Campaign: a grouping of coordinated adversarial behaviours that describe a set of malicious activities that occur over a period of time against one or more specific targets.
- (h) Compromise: violation of the security of an information system.
- (i) Confidentiality: property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
- (j) Course of action (Coa): an action or actions taken to either prevent or respond to a cyber incident.
- (k) Cyber: relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
- (l) Cyber alert: notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems.
- (m) Cyber event: any observable cyber occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
- (n) Cyber incident: a cyber event that jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
- (o) Response plan: procedures to respond to and limit consequences of a cyber incident.
- (p) Cyber resilience: the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
- (q) Cybersecurity risk: the combination of the probability of cyber incidents occurring and their impact.

- (r) Cyber security: preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium.
- (s) Cyber threat: a circumstance with the potential to exploit one or more vulnerabilities that can adversely affect cybersecurity.
- (t) Data breach: compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.
- (u) Defence-in-depth: security strategy integrating human resources, processes and technology to establish a variety of barriers across multiple layers and dimensions of an organisation.
- (v) Denial of service (DoS): prevention of authorised access to information or information systems, or the delaying of information system operations and functions, with a resultant loss of availability to authorised users.
- (w) Detection (function): develop and implement the appropriate activities to identify the occurrence of a cyber event.
- (x) Distributed denial of service (DDoS): a denial of service that is carried out using numerous sources simultaneously.
- (y) Exploit: defined way to breach the security of information systems through vulnerability.
- (z) Identification (function): develop an organisational understanding to manage cyber risk to assets and capabilities.
- (aa) Identity and access management (IAM): encompasses people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.
- (bb) Incident response team (IRT): team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.
- (cc) Indicators of compromise (IoC): identifying signs that a cyber incident may have occurred or may be occurring.
- (dd) Information sharing: an exchange of data, information and/or knowledge that can be used to manage risks or respond to events.
- (ee) Information system: a set of applications, services, information technology assets or other information-handling components, which includes the operating environment.
- (ff) Integrity: property of accuracy and completeness.

- (gg) Logical access: providing an authorised user the ability to access one or more computer-system resources such as a workstation, network, application, or database through automated tools.
- (hh) Malware: software designed with malicious intent, containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
- (ii) Material incident: any incident that is considered to have a major or significant impact on the operations of an institution and is likely to cause potential systemic failures.
- (jj) Multi-factor authentication: the use of two or more of the following factors to verify a user's identity: knowledge factor, possession factor and biometric factor.
- (kk) Non-repudiation: ability to prove the occurrence of a claimed event or action and its originating entities.
- (ll) Patch management: the systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.
- (mm) Penetration testing: a test methodology in which assessors, using all available documentation (for example, system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
- (nn) Protection (function): to develop and implement appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents.
- (oo) Recover (function): to develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired by a cyber incident.
- (pp) Recovery-point objectives (RPOs): refers to the amount of data that can be lost within a period most relevant to a business, before significant harm occurs, from the point of a critical event to the most preceding backup.
- (qq) Recovery-time objectives (RTOs): the amount of time that an application, system or process, can be down for without causing significant damage to the business as well as the time spent restoring the application and its data.
- (rr) Reliability: property of consistent intended behaviour and results.
- (ss) Respond (function): to develop and implement the appropriate activities to respond to a detected cyber event.
- (tt) Situational awareness: the ability to identify, process and comprehend the critical elements of information through a cyber-threat intelligence process that provides



a level of understanding that is relevant to act upon in mitigating the impact of a potentially harmful event.

- (uu) Social engineering: a general term for trying to deceive people into revealing information or performing certain actions.
- (vv) Tactics, techniques and procedures (TTPs): the behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
- (ww) Threat actor: an individual, a group or an organisation believed to be operating with malicious intent.
- (xx) Threat assessment: process of formally evaluating the degree of threat to an organisation and describing the nature of the threat.
- (yy) Threat intelligence: Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.
- (zz) Threat-led penetration testing (TLPT) (also known as red team testing): a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques, and procedures of real-life threat actors. It is based on targeted threat intelligence and focusses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.
- (aaa) Threat vector: a path or route used by the threat actor to gain access to the target.
- (bbb) Traffic light protocol (TLP): a set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established colour code to indicate expected sharing boundaries to be applied by the recipient.
- (ccc) Verification: confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
- (ddd) Vulnerability: a weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.
- (eee) Vulnerability assessment: systematic examination of an information system and its controls and processes to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

## **4. CYBER RISK MANAGEMENT AND OVERSIGHT**

### **(a) GOVERNANCE**

- 4.1 The governance domain comprises three elements: cyber-resilience strategy, cyber-resilience framework, and board and senior management responsibilities.

#### **(i) Cyber-Resilience Strategy**

- 4.2 A cyber-resilience strategy entails detailed plans of how an institution ensures that its assets are secured, thereby minimising cyber risk. The cyber-resilience strategy should be regularly reviewed to match the prevailing and evolving cyber-security landscape.
- 4.3 An institution should document its cyber-resilience strategy and ensure that, at the least, the following are considered:
- (a) the importance of cyber resilience to the institution and its key stakeholders;
  - (b) the institution's vision and mission in relation to cyber resilience;
  - (c) the cyber-resilience objectives that the institution will pursue;
  - (d) the institution's cyber risk appetite, to ensure it remains consistent with the institution's risk tolerance as well as the institution's overall business objectives and corporate strategy;
  - (e) a roadmap or implementation plan with change delivery and planning capabilities relating to people, processes and technology. The strategy should clearly set out how this roadmap or implementation plan will be delivered and how the board and senior management should track and monitor delivery;
  - (f) an institution must ensure that the cyber-resilience strategy is aligned to its corporate strategy and other relevant strategies; and
  - (g) an institution's board must approve the cyber-resilience strategy and ensure that it is regularly reviewed and updated according to the institution's threat landscape.
- 4.4 An institution should establish an internal cross-disciplinary steering committee comprising senior management and appropriate staff from different business units (for example, information technology (IT), legal, people, procurement, audit, and risk) to collectively develop a cyber strategy.
- 4.5 The steering committee should
- (a) provide multiple views and perspectives to ensure that the strategy is holistic and focusses on all elements related to people, processes and technology.
  - (b) evaluate and prioritise internal and external stakeholder needs and expectations, deciding on the overall requirements from cyber resilience.
  - (c) provide direction to senior management on what cyber resilience should achieve.

- (d) define who makes cyber-resilience decisions and how those decisions should be made.
- (e) consider an institution's risk tolerance when defining how cyber risks should be addressed.
- (f) evaluate how the different business units are affected and can work together in an integrated manner to achieve enterprise-wide outcomes.
- (g) consider how to monitor the performance and outcomes of cyber resilience and intervene if necessary to ensure that the specified direction is followed.

#### **(ii) Cyber-Resilience Framework**

- 4.6 An institution should have a cyber-resilience framework that clearly sets out how it determines its cyber-resilience objectives and risk tolerance, as well as how it effectively identifies, mitigates and manages its cyber risk to support objectives.
- 4.7 The framework should incorporate requirements (that is, policies, procedures and controls) related to governance, identification, protection, detection, response and recovery, testing and situational awareness.
- 4.8 An institution can use any of the recognised international and industry-level standards, guidelines and frameworks reflecting current industry best practices as a benchmark for designing its framework. Such standards include ISO/IEC 27001, COBIT 5, NIST CSF, ISF and other industry standards.
- 4.9 The framework should align with the formulated cyber-resilience strategy that is consistent with the enterprise risk management framework. Such consistency recognises that a bank's cyber-resilience framework is likely to share elements with the policies, procedures and controls that it has established to manage other risk areas.
- 4.10 A bank's cyber-resilience framework should clearly define the roles and responsibilities for managing cyber risk in emergencies and crises.

#### **(iii) Board and Senior Management Responsibilities**

- 4.11 The board and senior management are responsible for ensuring that cyber-security risk is effectively managed within an institution. The board should
  - (a) be responsible for approving a cyber-resilience strategy and framework, setting a bank's risk tolerance for cybersecurity risks and closely overseeing the bank's implementation of its cyber-resilience framework and the policies, procedures and controls that support it.
  - (b) be regularly apprised of a bank's cyber-security risk profile to ensure that it remains consistent with the bank's risk tolerance and overall business objectives. As the board shares this responsibility, it should consider how material changes to the bank's products, services, policies or practices, and the threat landscape affect its cyber-risk profile.

- 4.12 To carry out the foregoing responsibilities, a bank's board should ensure that it collectively possesses the appropriate balance of skills, knowledge and experience to understand and assess the cyber-security risks facing the bank. It should also be sufficiently informed and capable of credibly challenging the recommendations and decisions of designated senior management.
- 4.13 Senior management should
- (a) closely oversee a bank's implementation of its cyber-resilience framework, and the policies, procedures and controls that support it.
  - (b) cultivate a strong level of awareness and commitment to cyber resilience. An institution's senior management should promote a culture that recognises that staff at all levels have important responsibilities for ensuring the institution's cyber resilience and lead by example.
  - (c) ensure that behavioural and cultural change is nurtured and conveyed through leadership and vision with clear and effective messages.
  - (d) ensure that situational awareness materials are made available to relevant employees to mitigate cyber incidents, changes to the threat landscape and effects of these threats on the institution.
  - (e) ensure that a cyber-security function is established. The function must be independent of an institution's information technology function; to avoid any conflict, the cyber-security function must have a separate reporting function from the information technology function, separate budget and resources.
  - (f) ensure that a full-time senior manager for the cyber-security function, often referred to as chief information security officer (CISO)<sup>1</sup> is appointed at senior management level. CISO should be independent, possess an appropriate balance of skills, knowledge and experience, and have sufficient resources and direct access to the board. In addition, CISO should be responsible and accountable for implementing the cyber-resilience strategy and framework at the enterprise level.
  - (g) embed a programme for talent recruitment, retention, and succession planning for the staff.
  - (h) produce a formal cyber code of conduct that can be incorporated into an institution's code of conduct.
  - (i) continuously review skills<sup>2</sup>, competencies and training requirements to ensure that an institution maintains the right set of skills as technologies and risks evolve.

---

<sup>1</sup> This will vary depending on the size and complexity of an institution; for small institutions, the assessment may be at a manager level and report directly to a senior executive with access to the board.

<sup>2</sup> It is important that the board has at least one member who is competent in matters of cybersecurity.

- (j) develop key performance indicators, key risk measures and ensure supporting data is routinely collected at senior management level to monitor, measure and report on the implementation, effectiveness, consistency and persistence of cyber activities within an institution, the group and local financial system.
- (k) ensure the standard board information pack includes a report and metrics that cover cybersecurity. Sufficient time must be allocated to discuss issues on the board agenda.
- (l) ensure that an independent risk management function exists at an enterprise level. An independent risk management function ensures that the cyber-risk management framework has been implemented according to policy and consistently to an institution's risk appetite and tolerance. In addition, an independent risk management function reports significant changes in an institution's risk exposure to the appropriate governing authority.<sup>3</sup>
- (m) ensure that an independent audit function exists at an enterprise level. An independent audit function ensures the effective functioning of internal controls and applicable laws and regulations; updates its procedures to adjust to the evolving cyber threat landscape; and identifies, tracks, and reports significant changes in an institution's cyber-risk exposure to the appropriate governing authority.
- (n) establish processes to identify and communicate all cyber-security-related regulations and requirements. The process for ensuring compliance should be reviewed and updated when new regulatory requirements become effective. The regulatory compliance<sup>4</sup> process should address compliance with the following:
  - (i) payment card industry, data security standard (PCI-DSS)
  - (ii) SWIFT customer-security controls framework
  - (iii) electronic communications and transactions regulations
  - (iv) electronic evidence regulations
  - (v) Data Protection Act, Act No. 32 of 2018
  - (vi) Cybercrime and Computer Related Crimes Act, 2018
  - (vii) Banking Act (Cap. 46:04), and all other laws governing protection, integrity and availability of critical assets.

## 5 CYBER-SECURITY FUNDAMENTAL ELEMENTS

5.1 For completeness, a cyber-risk management framework should encompass a spectrum of fundamental elements, which are the subject of this section.

### (a) IDENTIFICATION

5.2 The identification function outlines areas institutions should address:

<sup>3</sup> The governing authority may be a risk committee comprising senior management, the board or a committee of the board.

<sup>4</sup> Regulatory compliance may differ according to the operations of an institution; some institutions may need to comply with other regulations not included in the guidelines.



**(i) Asset Management**

**5.3 An institution should**

- (a) maintain up-to-date inventory of all the critical functions; key roles; processes; information assets; third-party service providers and interconnections; and, where possible, automated tools should be used for this purpose. In determining the criticality of the information assets, an institution should at a minimum consider the confidentiality, integrity and availability principles of information security.
- (b) create and maintain a simplified network map of resources with an associated plan addressing internet protocol addresses, which locate routing, and security services and servers supporting critical functions and which identify links with the outside world.
- (c) maintain a comprehensive inventory of all individuals and systems accounts so that they can be aware of the access rights to information assets and their supporting systems; the inventory must be reviewed and updated regularly.
- (d) maintain up-to-date and complete maps of network resources, interconnections and dependencies, and data flows with other information assets, including the connections to business partners, internet-facing services, cloud services and any other third-party systems.

**(ii) Risk Assessment**

**5.4 An institution should**

- (a) understand cyber-security threats to institutional operations (including mission, functions, image, or reputation), institutional assets, and individuals. Asset vulnerabilities, as well as threats, both internal and external, should be identified and documented. Risk responses should be identified and prioritised and risk tolerance should be determined and the risk management processes should be established, managed, and agreed to by all those charged with the management of cyber risk.
- (b) use the risk management framework to identify risks and regularly conduct risk assessments of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections to determine, classify and document the institution's level of criticality.
- (c) embed risk assessment in project management methodology; risk assessment must be conducted at early stages of a project when deploying new technologies, products, services, and connections, to enable identification of potential threats and vulnerabilities. It should update its risk assessment in case new information affecting cyber risk is identified. The result of the risk assessment should feed into the cybersecurity strategy and framework.
- (d) identify cybersecurity risks that it bears from or poses to entities in its ecosystem and coordinate with relevant entities as appropriate.

**(b) PROTECTION**

5.5 An institution should consider the following measures to address the requirements of the protection function:

**(i) Identity and Access Management**

5.6 An institution should

- (a) identify and restrict physical and logical access to its system resources to the minimum required for legitimate and approved work activities, according to the principle of least privilege and separation of duties.
- (b) establish policies, procedures and controls that address access privileges and how that access should be administered. The information system access should be evaluated regularly to identify unneeded access or privileges. Physical, logical and remote access to critical systems should restrict and block any unauthorised access. Administration rights on systems should be strictly limited to operational needs.
- (c) establish and administer user accounts in accordance with a role-based access control (RBAC) scheme that organises allowed information system access rights and privileges into roles.
- (d) establish processes to manage the creation, modification or deletion of user access rights. Such actions should be submitted to and approved by appropriate staff and should be recorded for review if necessary.
- (e) implement specific procedures to allocate privilege access on a need-to-use or an event-by-event basis. Administrators should have two types of accounts: one for general purpose use and one to carry out their administrative tasks. The use of privileged accounts should be tightly monitored and controlled.

**(ii) Security Awareness and Training**

5.7 An institution should

- (a) ensure that its employees have a good understanding of the cyber-security risk they might face when performing their jobs and that they understand their roles and responsibilities in protecting the institution's assets.
- (b) provide its entire staff (permanent employees, temporary employees and contractors) with training to support cyber-security-policy compliance and the incident-reporting process. Training should include good practices for dealing with potential cyber incidents, including how to report unusual activity. Cyber-security awareness training should be part of the on-boarding programme for new staff.
- (c) ensure that before going into service operations, staff operating new systems should receive appropriate user training and be familiar with the operating procedures.

- (d) should validate the effectiveness of its training, assess whether the training and awareness positively influence behaviour and ensure that staff comply with the operating procedures. High-risk staff should be identified and receive dedicated security-awareness training that is relevant to their responsibilities.

(iii) **Human Resource Security**

5.8 An institution should

- (a) embed cybersecurity at each stage of the employment life cycle, specifying security-related action required during the induction of each employee and their ongoing management, and upon the termination of employment.
- (b) carry out background security vetting of all candidates that is commensurate with their future role and depending on the criticality of the assets and information they might have access to in order to fulfil their duty. Responsibilities for cybersecurity should be clearly stated in employment contractual agreements.
- (c) establish policies, procedures and controls for granting or revoking employees' physical and logical access to its systems, considering job responsibilities, principles of least privilege and segregation of duties.
- (d) establish capabilities, including people, processes and technologies to monitor privileged user activity and access to critical systems in order to identify and deter anomalous behaviour and notify appropriate staff.
- (e) monitor and analyse behaviour to identify anomalous activities and evaluate the implementation of innovative solutions to support detection and response to insider threat activity.
- (f) ensure that all access rights that are related to employees' previous position and are no longer necessary for their new responsibilities are revoked when employee responsibilities change. Employees in sensitive positions should be pre-screened to ensure due diligence and to protect the institution's information assets.

- 5.9 Senior management should ensure that the institution's cultural awareness of cybersecurity risk improves continuously across the organisation and its ecosystem. In addition, institutions should develop key indicators to measure the effectiveness of training programmes to ensure that there are updated regularly to take account of the evolving threat landscape to the ecosystem.

(iv) **Network and Infrastructure Management**

5.10 An institution should

- (a) implement a defence-in-depth security architecture based on the network and data flow diagrams that identify hardware, software and network components, internal and external connections and type of information exchanged between systems.

- (b) establish a baseline system and security configuration for information systems and system components, including devices used for accessing an institution's network remotely, to help the configuration and security reinforcements of those systems and components to be applied consistently. These baselines should be documented, formally reviewed and regularly updated to adapt to the institution's evolving threat landscape.
- (c) segment its network infrastructure with security policies appropriate to its use and commensurate with the risk score, which defines proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated using network management.
- (d) implement technical measures to prevent the execution of unauthorised code on institution-owned or managed devices, network infrastructure and system components and unauthorised devices should be prevented from connecting to the institution's networks.
- (e) develop appropriate controls to protect data at rest, in use and in transit. The controls should be commensurate with the criticality and the sensitivity of the data held, used or being transmitted, according to the risk assessment conducted in the identification function.

**(v) Systems Acquisition and Development**

**5.11 An institution should**

- (a) develop and implement a process governing the acquisition, development and maintenance of ICT systems; this process should be designed using a risk-based approach.
- (b) ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.
- (c) ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.
- (d) have a method in place for testing and approving ICT systems before their first use; the method should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. The institution should also use test environments that adequately reflect the production environment.
- (e) test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.
- (f) implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems.

Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments.

- (g) ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.
- (h) implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation or configuration of the ICT systems comprehensively to reduce any unnecessary dependence on subject experts. Documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

5.12 An institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (for example, end-user computing applications) using a risk-based approach. The financial institutions should maintain a register of these applications that support critical business functions or processes.

#### **(vi) Change and Patch Management**

5.13 An institution should have policies, procedures and controls for change management, which should include criteria for prioritising and classifying the changes. Before any change, an institution should ensure that the change request is

- (a) reviewed to ensure that it meets business needs.
- (b) categorised and assessed for identifying potential risks and to ensure that it will not negatively affect confidentiality, integrity and availability as well as the institution's systems and data.
- (c) approved before it is implemented by the appropriate level of management.<sup>5</sup>
- (d) the change management process should be based on well-established and industry-recognised standards and best practices, for example COBIT 5.
- (e) an entity should consider building a segregated or separate environment that mirrors the production environment, allowing rapid testing and changes and patches to be implemented, and for providing for rapid fall-back when needed.

5.14 An institution should

- (a) have a comprehensive patch management policy and process that includes maintaining current knowledge of available patches, identifying appropriate patches for particular systems and analyzing impacts if installed, ensuring that patches are installed properly (for example, by applying the four-eyes principle) and tested prior to and monitored after installation, and documenting all associated procedures, such as specific configurations required. Policies, procedures and controls must make use of the information from the asset inventory management

---

<sup>5</sup> Institutions must establish a change approval board.



process described in the identification phase that provides information on the installed programs and binaries.

- (b) ensure that installation of new patches have approval from the appropriate management level.
- (c) have necessary procedures for recovering quickly when changes or patches fail. Any changes to the production environment must have an associated contingency plan, where applicable, and have policies and procedures to prohibit unapproved changes and patch installation to the information system.

(c) **DETECTION**

(i) **Anomalies and Events**

5.15 An institution should

- (a) develop appropriate capabilities, including personnel, processes and technology, to monitor and detect, in time, anomalous activities and events by setting appropriate criteria, indicators and triggers to enable alerts; the institution should understand the potential impact of the events.
- (b) use the results of the risk assessment performed in the identity function to define, consider and document the baseline profile of system activities to help detect deviation from the baseline.
- (c) ensure that its relevant staff are trained to be able to identify and report anomalous activities and events, and that roles and responsibilities for detection are well defined to ensure accountability.
- (d) develop and implement a mechanism that correlates all the network and systems alerts, and anomalous activity across its business units to detect multifaceted attacks. A process to collect, centralise and correlate event information from multiple sources and log analysis to continuously monitor the environment and detect anomalous activities and events should be established.
- (e) continuously monitor and inspect network traffic, including remote connections, endpoint configuration and activity, to identify potential vulnerabilities or anomalous events promptly.
- (f) continuously monitor connections with external service providers, devices and software.

5.16 An institution's monitoring and detection capabilities should support information collection for forensic investigation. To facilitate forensic investigation, an institution should ensure that its logs are backed up at a secure location with controls, to mitigate the risk of alteration.

**(d) TESTING**

- 5.17 Any institution requires a framework for testing cyber resilience; thus, an institution should establish and maintain a comprehensive testing programme as an integral part of its cyber-resilience framework. The testing programme should consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of the core components of the cyber-resilience framework.
- 5.18 An institution should incorporate risk-based elements in developing the comprehensive testing programme. This should be reviewed and updated regularly, taking account of the evolving threat landscape and the criticality of assets.
- 5.19 Tests should be undertaken by independent parties, whether internal or external.
- 5.20 An institution's board and senior management should incorporate lessons from the test results into the cyber-resilience framework to continually improve its cyber-resilience posture.
- 5.21 An institution should regularly, at least annually, test critical systems, applications and data recovery plans.

**(i) Vulnerability Management**

- 5.22 An institution should develop a documented and regularly updated vulnerability management process to classify, prioritise and remedy potential weaknesses identified at the stage of vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.
- 5.23 The vulnerability management programme should identify any type of exploitable weakness in critical functions.
- 5.24 An institution should conduct vulnerability scanning for its external-facing services and internal systems and networks periodically. Vulnerability assessments should be performed before any deployment or redeployment of new or existing services supporting critical functions, applications and infrastructure components for fixing weaknesses, consistently with existing change and release management processes.
- 5.25 An institution should
  - (a) develop, monitor and analyse metrics to assess the performance and effectiveness of its vulnerability management programme.
  - (b) consider discussing relevant test conclusions with other stakeholders to boost the cyber resilience of its ecosystem and the financial sector as a whole, as far as possible and under specific information-sharing arrangements.
  - (c) conduct quarterly vulnerability assessments on running services, applications and infrastructure components for compliance checks against regulations, policy and configurations, as well as for monitoring and evaluating the effectiveness of security controls to address the identified vulnerabilities.

**(ii) Scenario-Based Testing**

- 5.26 An institution should perform different scenario-based tests, including extreme but plausible scenarios, to evaluate and improve its incident-detection capability, as well as response, resumption and recovery plans. Scenario-based tests can take the form of desktop exercises or simulations.
- 5.27 An institution's board and senior management should be engaged in the scenario-based test, when appropriate, to have them aware of the threat landscape and be able to reach risk-based decisions relating to, among others, resources and processes required to mitigate cyber threats.
- 5.28 To improve an institution's staff awareness and enhance the risk culture within an organisation, scenario-based tests should include social engineering and phishing simulation.
- 5.29 An institution should test the extent to which internal skills, processes and procedures can adequately respond to extreme but plausible scenarios, with a view to achieving stronger operational resilience.
- 5.30 An institution should form collaborative arrangements with the ecosystem to develop cybersecurity-incident scenarios involving significant financial loss and use them for stress tests to better understand potential spillovers and contagion risk to the ecosystem. The stress-test results should be used to further improve the institution's cyber-resilience stance.

**(iii) Penetration Tests**

- 5.31 An institution should
- (a) conduct penetration tests on its external-facing services and internal systems and networks to identify vulnerabilities in the adopted technology, organisation and operations regularly, or at least on an annual basis. Penetration tests should be conducted using a risk-based approach and, at the very least, in cases of major changes and new system deployment.
  - (b) perform penetration tests engaging all critical internal and external stakeholders in the penetration-testing exercises: system owners, business continuity, and incident and crisis response teams.
  - (c) design and perform penetration tests to simulate realistic attack techniques on systems, networks, applications and procedures.

**(iv) Red-Team Testing**

- 5.32 An institution should conduct red-team exercises<sup>6</sup> to test critical functions for possible vulnerabilities and the effectiveness of an institution's mitigating controls, including

---

<sup>6</sup> An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organisational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organisation.

controls relating to protection of personnel, processes and technology. It should also conduct independent red-team exercises, using regulatory and industry frameworks.

**(e) RESPONSE AND RECOVERY**

**(i) Cyber-resilience Incident Management**

- 5.33 An institution should develop a comprehensive cyber-incident response, resumption and recovery plans to manage cybersecurity events or incidents in a way that limits damage and prioritises resumption and recovery actions to facilitate the processing of critical transactions, increase the confidence of external stakeholders, and reduces recovery time and costs. Such plans should define policies and procedures as well as roles and responsibilities of escalating, responding to, and recovering from cyber-security incidents. An institution should ensure that all relevant business units are integrated into the plans.
- 5.34 The cyber-incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations.
- 5.35 An institution should
- (a) ensure that its incident response team has the requisite skills and training to address cyber incidents.
  - (b) after consideration of its critical function, key roles, processes, information assets, third-party service providers and interconnections, plan for how to operate in a diminished capacity or how to safely restore services over time, taking into consideration the relative priorities of services affected by the incident, and with accurate data. To make the best decisions about its recovery objectives after a cyber incident, an institution must first define its recovery-point objectives (RPOs) and its recovery-time objectives (RTOs) commensurate with its business needs and systemic role in the ecosystem.
  - (c) regularly (quarterly) test its cyber contingency, response, resumption and recovery plans against a range of different plausible scenarios.
  - (d) define alert indicators and thresholds for detecting cyber-security incidents that trigger the incident management processes and procedures, which, in turn, include alerting and conveying information to the appropriate staff.
  - (e) have processes and procedures for collating and reviewing information from its cyber-security incidents and testing results in order to continuously improve its contingency, response, resumption and recovery plans.
  - (f) have processes and procedures to conduct an ex post root-cause analysis of its cyber-security incidents. Findings of the root-cause analysis should be incorporated into the cyber response, resumption and recovery plans.

**(ii) Data Integrity**

5.36 An institution should

- (a) develop a formal backup policy specifying the minimum frequency and scope of data, taking into consideration data sensitivity and the frequency with which that new information is introduced.
- (b) develop backup and recovery methods and strategies to be able to restore system operations with minimum downtime and limited disruption.
- (c) regularly back up all data necessary to replay participants' transactions.
- (d) store backup copies at an alternate site with a different risk profile to the main site and with transfer rates consistent with actual RPOs. The alternate site and backups should be safeguarded by stringent protective and detective controls.
- (e) back up its information system by maintaining a redundant secondary system that is not located in the same place as the primary system and that can be activated without information being lost or operations disrupted.
- (f) consider having a data-sharing agreement with third parties or participants to obtain uncorrupted accurate data from them for recovering its business operations in a timely manner.

5.37 Backups should be protected at rest and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and integrity.

**(iii) Communication and Collaboration**

5.38 An institution should

- (a) identify, document and regularly review systems and processes supporting its critical functions or operations that are dependent on external connectivity.
- (b) develop policies and procedures that define how it should work together with relevant interconnected entities to enable operations to be resumed (priority being its critical functions and services) as soon as it is safe and practicable to do so.
- (c) closely cooperate with its interconnected entities within the ecosystem, establishing roll-back processes to restore all its services accurately and safely. Moreover, an institution should test the effectiveness of these procedures regularly.
- (d) design its network connection infrastructure in a way that allows connections to be segmented or severed instantly to prevent contagion arising from cyber attacks.



**(iv) Crisis Communication and Responsible Disclosure**

- 5.39 This section discusses how a cyber-incident communication plan is developed and what elements are included in the plan, how information is collected in the field, analysed, and eventually disseminated to internal and external stakeholders in the media world that is evolving.
- 5.40 An institution should
- (a) identify and determine staff who are essential for mitigating the risk of a cyber incident and make them aware of their roles and responsibilities regarding incident escalation.
  - (b) establish criteria and procedures for escalating cyber incidents or vulnerabilities to the board and senior management, taking account of the potential impact and criticality of the risk.
  - (c) have a communication plan and procedures to notify, as required or necessary, all relevant internal and external stakeholders (including oversight, regulatory authorities, media and customers) promptly when it becomes aware of a cyber incident or when a cyber incident occurs. Incident reporting to the Bank of Botswana should be within 48 hours from detecting the incident.
  - (d) have a policy and procedures to enable potential vulnerabilities to be disclosed responsibly. In particular, it should prioritise disclosures that could help stakeholders to respond promptly and mitigate risk, which could benefit the ecosystem and broader financial stability.
  - (e) establish and regularly review information-sharing rules, agreements and modalities to control the publication and distribution of information that may have adverse consequences if disclosed.
  - (f) at least annually, test response, resumption and recovery plans, including governance and coordination, and crisis communication arrangements and practices. The incident response plan should identify the internal and external stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place.
- 5.41 The incident response plan should identify the internal and external stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place.

**(v) Supply Chain and Dependency Management**

- 5.42 An institution should maintain and regularly update an inventory of its participants and third-party service providers and ensure that its cyber-resilience framework addresses its interconnections with those entities from a cyber-risk perspective.
- 5.43 An institution's third-party risk assessment should be carried out regularly, taking into account the evolution of its threat landscape. It should, using a risk-based approach,

ensure that the provision of outsourced services is commensurate with the cybersecurity posture of the vendor.

5.44 An institution should

- (a) assess third-party service provider's security capabilities at least through third-party self-assessment.
- (b) obtain assurance of the third-party service provider's cyber-resilience capabilities and may use tools such as certification, external audits (for example, SOC 2), summaries of test reports, service level agreements (SLAs) and key performance indicators.
- (c) ensure that there are appropriate procedures to isolate or block its third-party connections (in a timely manner) if there is a cyber attack or a risk of contagion.

5.45 The independent audit function should validate an institution's third-party relationship management and outsourcing.

**(vii) Cyber Threat Intelligence**

5.46 An institution should

- (a) identify cyber threats that could materially affect its ability to perform or provide services as expected or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem.
- (b) have capabilities in place to gather cyber-threat information from internal and external sources (for example, application, system and network logs; security products such as firewalls and IDSs; trusted threat-intelligence providers; and publicly available information sources).
- (c) belong or subscribe to a threat and vulnerability information-sharing source or ISAC that provides information on cyber threats and vulnerabilities. Cyber-threat information gathered by an institution should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments that may trigger cyber attacks on any entity within an institution's ecosystem.
- (d) have the capabilities to analyse the cyber-threat information gathered from different sources, while taking into account its business and technical characteristics to
  - (i) determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which an institution is at risk of a targeted attack from them;
  - (ii) assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the institution; and

- (iii) analyse cyber-security incidents experienced by other organisations (where available), including types of incidents and origin of attacks, the target of attacks, preceding threat events and frequency of occurrence, and determine the potential risk these pose to the institution.

5.47 An institution should analyse the cyber-threat intelligence to produce relevant cyber-threat intelligence and continuously use it to assess and manage security threats and vulnerabilities for the purpose of implementing appropriate cyber-security controls in its systems and, at a more general level, enhance its cyber-resilience framework and capabilities on a sustained basis.

(viii) **Information Sharing**

5.48 An institution should

- (a) define the goals and objectives of information sharing in line with its business objectives and cyber resilience framework. At the very least, the objectives should include collecting and exchanging information in a timely manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber attack.
- (b) should define the scope of information-sharing activities by identifying the types of information available to be shared (for example, attackers' modus operandi, indicators of compromise, threats and vulnerabilities), the circumstances under which sharing this information is permitted (for example, in the case of a cyber incident), those with whom the information can and should be shared and how information provided to the institution and other sector participants will be acted upon.
- (c) establish and implement protocols for sharing information relating to threats, vulnerabilities and cyber incidents with employees, having regard to their specific roles and responsibilities.
- (d) have in place a process to access and share information with external stakeholders in a timely manner, such as regulators, law enforcement or other organisations within the institution's ecosystem.
- (e) establish and regularly review information-sharing rules and agreements and implement procedures that allow information to be shared promptly and in line with the objectives and scope as delineated above, while, at the same time, meeting its obligations to protect potentially sensitive data that may have adverse consequences if disclosed improperly.
- (f) participate actively in the Financial Sector Information Sharing and Analysis Centre (FS-ISAC), including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early-warning indicators relating to cyber threats.

## APPENDIX

### Appendix A: Cyber-security Incident Reporting Form

BANK OF BOTSWANA CYBER-SECURITY INCIDENT REPORTING FORM								
<b>Section A: General Information</b>		<b>REF NO:</b>						
<b>INSTITUTION/MM/DD/YY</b>								
<p>A1. Institution: choose Institution</p> <p>A2. Reporter's Contact Information:  <b>Full Names:</b> Click or tap here to enter text.  <b>Email Address:</b> Click or tap here to enter text.  <b>Telephone Number:</b>  <b>Date:</b> Click or tap to enter a date.</p> <p>A3. Is this a <input type="checkbox"/> New incident <input type="checkbox"/> Update to a reported incident?</p> <p>If it is an update on a reported incident provide a brief description of the incident.</p> <p>Click or tap here to enter text.</p> <p>A4. What category is this incident being classified as?</p> <table border="0"> <tr> <td>Category 1 <input type="checkbox"/></td> <td>Category 2 <input type="checkbox"/></td> <td>Category 3 <input type="checkbox"/></td> </tr> <tr> <td>Critical System Affected</td> <td>Incident occurred on network or system that could put critical system at risk</td> <td>Incident occurred on noncritical system</td> </tr> </table>			Category 1 <input type="checkbox"/>	Category 2 <input type="checkbox"/>	Category 3 <input type="checkbox"/>	Critical System Affected	Incident occurred on network or system that could put critical system at risk	Incident occurred on noncritical system
Category 1 <input type="checkbox"/>	Category 2 <input type="checkbox"/>	Category 3 <input type="checkbox"/>						
Critical System Affected	Incident occurred on network or system that could put critical system at risk	Incident occurred on noncritical system						
<b>Section B: Incident</b>								
<p>B1. Types of threat/incident (You may choose more than one item)</p> <p><input type="checkbox"/> Denial of service (DoS)</p> <p><input type="checkbox"/> Virus/worm/Trojan</p> <p><input type="checkbox"/> Website defacement</p> <p><input type="checkbox"/> Ransomware</p> <p><input type="checkbox"/> Intrusion/hack/unauthorised access</p> <p><input type="checkbox"/> Distributed denial of service (DDoS)</p> <p><input type="checkbox"/> Misuse of systems/inappropriate usage</p> <p><input type="checkbox"/> Other: Click here to enter text.</p> <p>B2. Is this incident related to another incident previously reported? Choose an item.</p> <p>If "yes", provide more information on how both incidents are related. Click or tap here to enter text.</p> <p>Please provide the reference no. of the previously reported incident. Ref no: Click here to enter text.</p>								

**Section C: Incident Details**

C1. Please provide details of the incident in the box below.

When was the incident first observed?

Click or tap to enter a date.

How was the incident first observed/sighted/detected?

Click here to enter text.

C2. Please provide details of the critical system(s) or network(s) that is/are impacted by this incident. Details should minimally include:

*-Location, the purpose of this system/ network, affected applications (including hardware manufacturer, software developer, make/ model, etc.) running on the systems/ networks, etc.*

Click here to enter text.

Where relevant, please indicate the operating system of the affected critical system(s): Choose an item.

- If others, kindly state the OS: Click here to enter text.

C3. What is the impact of the attack? (Tick 'one' checkbox for each column)

Service Delivery	(Loss of ) Sensitive Information	Public Confidence and Reputation
<input type="checkbox"/> No Impact	<input type="checkbox"/> No loss	<input type="checkbox"/> No Impact
<input type="checkbox"/> Minor Impact	<input type="checkbox"/> Minor Loss	<input type="checkbox"/> Minor Impact
<input type="checkbox"/> Major Impact	<input type="checkbox"/> Major Loss	<input type="checkbox"/> Major Impact
<input type="checkbox"/> Serious Impact	<input type="checkbox"/> Serious Loss	<input type="checkbox"/> Serious Impact
<input type="checkbox"/> Severe Impact	<input type="checkbox"/> Severe Loss	<input type="checkbox"/> Severe impact

C4. Does the affected critical system(s)/ network(s) have a potential impact on another critical asset(s) of the financial Institution?

Choose an item.

If "yes", please provide more details.

Click here to enter text.

C5. Can the affected system have a systemic impact? If yes, provide details

Click or tap here to enter text.

**Section D: Incident Handling Status**

D1. What follow-up action(s) have been taken at this time?

Click or tap here to enter text.

D2. What is the current status or resolution of this incident?

Choose an item.

If it is not resolved, what is the next course of actions?

Click here to enter text.

D3. What is the source/cause of the incident? ('NIL' OR 'NA' if unknown)

Click here to enter text.

D4. Has the incident been reported to any law enforcement?

Choose an item.

If "yes", specify the agency that is being reported to.

Click or tap here to enter text.



**Section E: Other Information****E1. IP addresses** *(Required if surfaced from the incident)*

Provide the list of IP addresses surfaced from incident. Please state the involvement of the IP addresses in the incident (for example, victim, malware command & control servers, etc.). If IP addresses were resolved from domain names, please specify the domain names and the date/time of resolution of IP addresses from the domain names.

IP Address	Involvement	Domain name from which IP address was resolved	Date/time of resolution of IP address from domain name

**E2. Domain Names** *(Required if surfaced from the incident)*

Provide the list of domains surfaced from incident. Please state the involvement of the domain names in the incident. (for example, drive-by-download servers, malware control & command servers, defaced website)

Domain Name	Involvement of Domain name

**E3. Email addresses** *(Required if surfaced from the incident)*

Provide list of email addresses surfaced from incident. Please state the involvement of the email addresses in the incident. For example, email address from which a phishing email appeared to be sent from, etc.

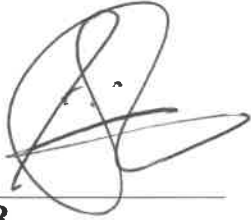
Email Address	Involvement of Email Address

**E4. Malicious files** *(Required if surfaced from the incident)*

Provide information on the malicious files surfaced in the incident in the box below.

Filename	Size	MD5 hash	Technical Analysis (Yes/No)

Issued this 31<sup>st</sup> day of May 2023

A handwritten signature in black ink, consisting of a large, stylized 'E' or 'G' shape with a horizontal line extending to the right.

**DIRECTOR**  
**PRUDENTIAL AUTHORITY AND PAYMENTS OVERSIGHT DEPARTMENT**