



10 December 2021

Circular Number 42 of 2021

To: Insurance Companies

Brokers

Reinsurers

Pension Funds

Pensions Fund Administrators

Cc: Life Offices Association (LOA)

Insurance Council of Zimbabwe (ICZ)

Zimbabwe Association of Reinsurance Organisations (ZARO)

Zimbabwe Association of Pension Funds (ZAPF)

Zimbabwe Association of Funeral Assurers (ZAFA)


Insurance Brokers Association of Zimbabwe (IBAZ)

**INVITATION FOR COMMENTS ON THE DRAFT RISK-BASED CYBERSECURITY AND
DATA PROTECTION FRAMEWORK FOR THE INSURANCE AND PENSIONS
INDUSTRY IN ZIMBABWE**

1. The Insurance and Pensions Commission has developed a draft Risk-Based Cybersecurity and Data Protection Framework for the Insurance and Pensions industry to provide guidance in the implementation of cybersecurity programmes for enhancing the industry's resilience sustainability.
2. The rising concerns around cybersecurity have necessitated the formulation of this cybersecurity framework, to address the numerous risks posed by cyber-attacks.
3. The draft Risk-Based Cybersecurity Framework provides a risk-based approach to managing cybersecurity risk.

4. We therefore request that all regulated entities go through the draft framework attached and provide their comments to the Commission no later than 17 January 2022.
5. May you kindly direct all comments and clarifications on the draft to actuarial@ipecc.co.zw.
6. Your usual cooperation will be greatly appreciated

Yours sincerely



Grace Muradzikwa

COMMISSIONER OF INSURANCE, PENSION AND PROVIDENT FUNDS

INSURANCE AND PENSIONS COMMISSION



Risk Based Cybersecurity and Data Protection Framework for the Insurance and Pensions Industry in Zimbabwe

21 October 2021

Contents

1. Definition of Terms.....	4
2. Introduction and background.....	5
3. Objectives	6
4. Scope of Application and Effective Date	7
5. Cybersecurity Strategy and Framework.....	7
6. Governance and Board Oversight	9
7. Risk Management System.....	15
8. Monitoring.....	Error! Bookmark not defined.
9. Response and Recovery	Error! Bookmark not defined.
10. Training and Awareness.....	Error! Bookmark not defined.
11. Reporting.....	21
12. Compliance	21

DRAFT

AUTHORISATION

This Risk-Based Cybersecurity Framework for the Insurance and Pensions Industry is issued in terms of Section 3(1)(c) of the Insurance and Pensions Commission (Issuance of General Guidelines and Standards) Regulations, 2020 published in Statutory Instrument 69 of 2020, which empowers the Commission to issue guidelines and standards to govern risk management and corporate governance practices to be observed by the insurance and pension industry.

DRAFT

ACROYMNS

BCP	Business Continuity Plans
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
FATF	Financial Action Task Force
HoIT	Head of Information Technology
IAIS	International Association of Insurance Supervisors
ICPs	Insurance Core Principles
ICT	Information and Communication Technology
IOPS	International Organisation of Pension Supervisors
IOSCO	International Organization of Securities Commissions
IPEC	Insurance and Pensions Commission
ISC	Information Security Committee
IT	Information Technology
OECD	Organisation for Economic Co-operation and Development
RPO	Recovery Point Objective
RTO	Recovery Time Objective

1. DEFINITION OF TERMS

In this Framework:-

“Business Continuity Plan” means a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organisation in the event of a disruption;

“Cybersecurity” means an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation;

“Cyber risk” means any risk arising from a failure of an entity's information technology systems resulting in financial loss, disruption of services, and interference with business as usual, or damage to the reputation of an entity;

“Cyber resilience” means the ability of a regulated entity to—

- a) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and
- b) recover to effective operational capability in a time frame consistent with the provision of critical economic services;

“Cybersecurity incident” refers to an event that threatens the security of the system of a regulated entity which shall include leakage of data in electronic form, denial of service attack, compromise of protected information systems or data assets, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems;

“Designated Information Security Function” shall be responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected;

“Risk-based Cyber Risk Management” means an approach whereby regulated entities identify, assess and understand the risks to which they are exposed to and take effective measures commensurate with these risks;

“Regulated entity” means insurance companies, brokers, reinsurers, pension funds, and fund administrators registered by the Commission;

“System” means any data, hardware, software, network, or other information technology component which is part of an IT infrastructure.

2. INTRODUCTION AND BACKGROUND

2.1 This Guideline is issued by the Insurance and Pensions Commission (hereinafter referred to as “IPEC” or “Commission”) to provide guidance in the implementation of regulated entities’ cybersecurity programmes for enhancing their resilience sustainability.

2.2 This guideline is issued in line with IPEC’s mandate of regulating and supervising the insurance and pensions industry for the protection of existing and potential policyholders and pension and provident funds members.

2.3 The guideline was prepared in line with international best practices set out by the International Associations of Insurance Supervisors (IAIS), International Organisation of Pension Supervisors (IOPS) and Organisation for Economic Cooperation and Development (OECD).

2.4 IAIS Insurance Core Principles (ICPs) broadly highlight areas that insurance companies should address regarding cyber risk and cyber resilience through management of significant risks and related internal controls, and the relevant ICPs include:

- ICP 7 Corporate Governance
- ICP 8 Risk Management and Internal Controls
- ICP 9 Supervisory Review and Reporting
- ICP 19 Conduct of Business
- ICP 21 Countering Fraud in Insurance

2.5 Similarly, the OECD and IOPS also underscore issues of corporate governance, risk management, and internal controls for pension funds and fund administrators. Cybersecurity falls with the operation and outsourcing risks arising from inadequate or failed internal processes,

people, and systems, including IT systems, as well as the risks related to the outsourcing of business activities.

- 2.6 Cybersecurity must be fully integrated into business goals and objectives and be an integral part of the overall risk management processes for it to be effective. Cybersecurity needs to be addressed at all levels of an entity and with respect to relevant third-party arrangements.
- 2.7 The increased adoption of information technologies by regulated entities exacerbates cybersecurity threats, both in frequency and sophistication.
- 2.8 Cybersecurity is among the predicate offences listed by the Financial Action Task Force (FATF). FATF (2020) observed an increase in money laundering and terrorist financing risks stemming from Covid-19-related crimes, which include increased misuse of online financial services and virtual assets to move and conceal illicit funds.
- 2.9 The concerns around cybersecurity have necessitated the formulation of cybersecurity framework to address the numerous risks posed by cyber-attacks.
- 2.10 This Risk-Based Cybersecurity Framework for the Insurance and Pensions Industry provides a risk-based approach to managing cybersecurity risk.
- 2.11 This Framework document comprised of six parts:
 - i. Cybersecurity Strategy and Framework,
 - ii. Governance and Board Oversight,
 - iii. Cybersecurity Risk Management System,
 - iv. Response and Recovery, Monitoring and
 - v. Reporting, and Training and Awareness.

3. OBJECTIVES

- 3.1 The objectives of the Framework are to ensure that regulated entities:
 - i. develop and implement cybersecurity procedures for enhancing cyber-resilience.
 - ii. have board approved cybersecurity strategies, frameworks, and policies in place.

- iii. are adequately prepared to prevent, mitigate, and address cybersecurity-related risks.
- iv. an in-built governance mechanism is in place for the effective implementation of the cybersecurity framework.

4. SCOPE OF APPLICATION AND EFFECTIVE DATE

- 4.1 The Framework applies to all insurance companies, brokers, reinsurers, pension funds, and fund administrators regulated by IPEC. In the case of pension funds, this Framework shall apply in full to stand-alone self-administered funds. For funds that outsource administration services, the Board shall evaluate the extent to which the systems applied by the service provider in order to be satisfied that they conform to the requirements stated in this Framework.
- 4.2 This Framework sets the minimum standards that IPEC regulated entities referred to in clause 4.1 must adopt to develop effective cybersecurity governance and risk management frameworks.
- 4.3 The Framework shall become operational with effect from XXXXXX.
- 4.4 The Commission reserves the right to amend this Framework from time to time.

5. CYBERSECURITY STRATEGY AND FRAMEWORK

- (a) Regulated entities must establish and maintain a cybersecurity strategy and framework tailored to prevent, mitigate and address relevant cyber risks that are commensurate with the nature, size, and complexity of their business.
- (b) The cybersecurity strategy and framework must be approved by the board of the regulated entity.

5.1. Cybersecurity Strategy

- 5.1.1. The Cybersecurity strategy must include well-defined processes and technology necessary for managing cyber risks and timely communication of the strategy with all users.

5.1.2. The strategy must address and mitigate cyber-risk while providing compliance with the statutory, contractual, and regulatory requirements.

5.1.3. The strategy must align with the entity's information technology and the overall corporate strategy.

5.1.4. The cybersecurity strategy must be reviewed at least annually. The review must also be done upon the occurrence of a cyber incident or major external cyber event which potentially could impact the entity, or upon the deployment of a new system.

5.2. Cybersecurity Framework

5.2.1. Regulated entities must have a cybersecurity framework, in support of their strategy, which aligns policies, business and technological approaches to address cyber risks.

5.2.2. The regulated entity's framework must maintain and promote the entity's ability to anticipate, detect, withstand, contain and recover from cybersecurity incidents, to limit the likelihood or impact of a cybersecurity incident, which could damage an entity's operations, reputation, and the data privacy of policyholders and third parties.

5.2.3. The regulated entity's cybersecurity framework must clearly define the entity's:

- i. cybersecurity objectives and coverage;
- ii. requirements for the competency of relevant personnel or system users; and
- iii. processes, and technology necessary for managing cyber risks and timely communication (including a plan for identification, assessment, measurement, monitoring, mitigation, and management of cyber risk).

5.2.4. The regulated entity's framework must be reviewed and updated at least annually to ensure that it remains effective.

5.2.5. Regulated entities may make reference to the best available and practicable quality assurance standards, taking into account their business nature, size, complexity, and risk profile.

5.3. Cybersecurity Policy

5.3.1. Every regulated entity must develop a cybersecurity policy, either as a separate document or as part of its cybersecurity framework or its Information Management Systems Policy.

5.3.2. The cybersecurity policy must be approved by the regulated entity's board and reviewed and updated at least annually or when there are significant changes in an entity's cyber-risk exposure. The annual review shall ensure suitability, adequacy, and effectiveness of the cybersecurity policy in mitigating cyber-risk.

6. GOVERNANCE AND BOARD OVERSIGHT

(c) Every regulated entity must have an effective governance structure that is fundamental for cybersecurity resilience, to help the entity to maintain a systematic and proactive approach to managing the prevailing and emerging cyber risks at all levels within the entity.

(d) As such, an entity should have clear cybersecurity governance rules which provide sound and prudent management and oversight of the entity's business.

6.1. The Board of Directors

(a) The Board of Directors of a regulated entity (hereinafter collectively referred to as "the board") shall hold the overall responsibility for cybersecurity controls and improvement of the organisation's governance framework for cybersecurity.

(b) The board shall be responsible for the following:-

- i. Setting strategy, formulating a cybersecurity policy and framework;
- ii. Approving the information and cyber security assessment programmes for evaluating the effectiveness of the existing cybersecurity framework; and

- iii. The board may delegate its primary oversight responsibility for cybersecurity controls and improvement of the entity's governance framework for cybersecurity to a risk management committee. However, this delegation shall not absolve the board of its said primary oversight responsibility.
- iv. Ensuring that the functions required to be executed in terms of this Framework are specifically assigned so as to ensure effective implementation and accountability for the functions.

6.2. Board Oversight

- (a) Entities should promote a risk-conscious culture through effective oversight, collaboration, and cooperation on cyber risk matters at the board level.
- (b) The board is responsible for the following cyber risk oversight responsibilities:-
 - i. Setting the tone from the top which fosters a robust cyber risk management culture.
 - ii. Ensuring that the cyber security policy aligns with the overall business strategy.
 - iii. Promoting awareness of and commitment to cybersecurity through creating a culture that recognizes that staff at all levels have important responsibilities in ensuring the entity's cybersecurity.
 - iv. Establishing an entity's vision, risk appetite, and overall strategic direction about cybersecurity.
 - v. Ensuring that cybersecurity activities are adequately budgeted for.
 - vi. Ensuring that the cybersecurity policy which incorporates monitoring metrics coupled with reporting and trend analysis is applied to all subsidiaries of the entities in different geographic regions.
 - vii. Incorporating cybersecurity as a standard agenda in board meetings.
 - viii. Reviewing and approving ICT strategic plan that aligns with the overall business strategy.

6.3. The Executive Management

- (a) Management of every regulated entity shall be responsible for implementing the business strategy, risk appetite, and threats.
- (b) Management shall also be responsible for closely overseeing the implementation of the entity's cyber resilience framework, including the policies, procedures, and controls.
- (c) The executive management shall be responsible for:-
 - i. Implementating the cybersecurity strategy, and framework approved by the board.
 - ii. Ensuring that the staff understands the organisational cyber risk profile.
 - iii. Clearly spelling out the Business Continuity Plans (BCP), strategies, Recovery Time Objective (RTO), and Recovery Point Objectives (RPO).
 - iv. Overseeing deployment of strong authentication measures to protect customer data, transactions, and systems.
 - v. Ensuring that staff members are subjected to enhanced background checks before being engaged.
 - vi. Overseeing the evaluation and management of risks introduced by third-party service providers.
 - vii. Collaborating with other entities and security agencies to share the latest cyber threats or attacks encountered by the entity.

6.4. Designated Information Security Function

- (a) Every regulated entity shall have designated information security function led by a suitably qualified and experienced Senior Level Officer who will be responsible for articulating and enforcing the policies to protect information assets.
- (b) The Head of Information Technology (HoIT) of an entity shall not preferably lead the information security function. Where either the HoIT or a senior person of the Information Technology department is

- appointed to lead the information security function, it must be ensured that direct reporting lines of that person for both the roles are separate.
- (c) The head of designated Information Security Function should have regular access to the risk management committee, sufficient authority, command of the subject matter, experience, and resources to fulfill his/her duties.
- (d) The Head of designated Information Security Function shall be responsible for:-
- i. Articulating the Information and cybersecurity policy for the entity.
 - ii. Providing advice and support to management and information users in the implementation of cybersecurity policy.
 - iii. Building and leading the information security team with appropriate competencies to deliver on the information security program.
 - iv. Promoting user awareness, carrying out day to day cybersecurity activities, and mitigating cybersecurity risk, and ensure that the entity maintains an enterprise-wide knowledge base of its users, devices, applications and their relationships, including but not limited to:
 - software and hardware asset inventory;
 - network maps (i.e. traffic and data flow); and
 - network utilisation and performance data.
 - v. Identifying and maintaining an updated log of individual system credentials relating to information access rights.
 - vi. Conducting regular professional cybersecurity related training to improve technical proficiency of staff.
 - vii. Ensuring that adequate processes for monitoring ICT systems, detecting cybersecurity threats and incidents on time are in place.
 - viii. Reporting to the CEO at least once per quarter on the following:
 - Assessment of the confidentiality, integrity, and availability of the information systems in the entity;
 - Assessment of the effectiveness of the approved cybersecurity program; and

- All material cybersecurity events that affected the entity during the period.
- ix. Ensuring timely update of the incident response mechanism and Business Continuity Plan (BCP).
- x. Ensuring frequent data backups of critical ICT systems and real-time backup of changes made to critical data.
- xi. Continuously testing disaster recovery and Business Continuity Plans (BCP) to ensure that the entity can continue to function and meet its regulatory obligations in the event of an unforeseen cyber-attack.
- xii. Creating a post incident analysis framework for preventing similar incidents in the future.

6.5. Information Security Committee

- (a) Every regulated entity must form an Information Security Committee (ISC) composed of members with the appropriate skills and knowledge on information security governance. The committee shall be headed by a senior level executive with a reporting line to the board. The members of ISC shall consist of senior representatives of relevant departments within the regulated entity. Secretary of the committee shall be the convener of the Information Security Committee.
- (b) The Information Security Committee shall be responsible for:-
 - i. Reviewing and recommending to the risk management committee necessary changes to the high level information security policy.
 - ii. Enforcing the implementation of policies for investment prioritisation and security risk management.
 - iii. Ensuring compliance to regulatory and statutory requirements related to information security.
 - iv. Providing strategic direction and cybersecurity governance for the entity.
 - v. Reporting to the risk management committee on information security activities

- vi. Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures

6.6. Independent Assessments

6.6.1. A regulated entity's governance, systems and processes for its ICT and cybersecurity risks should be audited on a periodic basis in line with the undertakings' audit plan by auditors with sufficient knowledge, skills and expertise in ICT and security risks to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the entity. The frequency and focus of such audits should be commensurate with the relevant nature, size, and complexity of their business.

a) Role of Internal Auditors

The Internal auditors of a regulated entity shall be responsible for:-

- i. Ensuring that entities incorporate cyber security reviews into their internal auditors' plan for the entity.
- ii. Conducting an audit for third party or vendors handling critical data on a planned basis or where necessary to measure the effectiveness of the third-party security controls implemented.
- iii. Communicating and discussing all instances of non-compliance related to Information security with relevant line management and CISO.

b) Role of External Auditors

The regulated entity must ensure that its external auditor's ICT audit scope includes but is not limited to the following:-

- i. Obtaining an understanding of the entity's ICT infrastructure, use of IT, operations, and the impact of ICT on financial reporting statements.
- ii. Understanding the extent of the entity's automated controls as they relate to financial reporting. This must include an understanding of:
 - ICT general controls that affect the automated controls;

- Reliability of data and reports used in the audit that is produced by the entity; and
- Comprehensive review of the approved cybersecurity strategy and policy.

7. RISK MANAGEMENT SYSTEM

7.1 Risk-Based Cyber Risk Management

- (a) Risk-based cyber risk management requires that the regulated entity has good knowledge or understanding of the threats and vulnerabilities in their ecosystem.
- (b) Regulated entities shall have a cybersecurity risk assessment approach that is commensurate with the security risks they are exposed to.
- (c) The Risk Management approach must be based on an understanding of threats, vulnerabilities, risk profile, and level of risk tolerance of the entity.
- (d) The regulated entity's systems and functions must be adequate for the nature, scale, and complexity of the entity business and cyber-risks.

7.2. Risk Management

- (a) Regulated entities must have, as part of institution wide risk management framework and governance requirements, effective systems of cyber-risk management and control measures to ensure consistent management of risks across the entity, and to reduce the incidence of significant adverse impacts on an entity by addressing threats, mitigating exposure, and reducing vulnerability.
- (b) Cybersecurity risk management should be continuous and proactive, requiring oversight, not only of the technology but also of the people and the processes that use and support the technology.
- (c) The risk management process shall also be dynamic given the constantly changing risk landscape.
- (d) The board and senior management of the regulated entity shall offer support and be involved in the cyber risk management process by

ensuring that the resources and capabilities are available and roles of staff are properly defined in the management of risks.

- (e) The Risk Management System shall entail five basic activities as stated below:
 - i. Risk Identification
 - ii. Risk assessment
 - iii. Risk measurement
 - iv. Risk mitigation/Risk treatment
 - v. Risk Understanding
- (f) Risk identification shall be done to identify and document asset and asset vulnerabilities. Regulated entities need to understand that it is almost impossible to protect everything, so they need to identify the assets that must be protected, and their priorities.
- (g) Risk assessment shall be done to identify and document internal and external threats to information technology assets. This involves the identification of potential sources of harm to the assets which need to be protected. Risk treatment options such as risk reduction, risk retention, risk avoidance, risk transfer, and how residual risk is addressed should be selected based on the outcome of the risk assessment.
- (h) Information obtained from risk management activities shall be reported to the senior management and the board of directors to support informed decision-making.

7.3. Role of Risk Management Function

- (a) The risk management function comprises risk control and compliance oversight functions which ultimately ensure that an entity's management of data, processes, risks, and controls are effectively operating.
- (b) The entity's risk management function includes but is not limited to:-
 - i) Assessing the risks and exposures related to cybersecurity and determining whether they are aligned to the entity's risk appetite.

- ii) Monitoring current and emerging risks and changes to legislation that may impact the level of cyber risk exposure in the entity.
- iii) Collaborating with system administrators and others responsible for safeguarding the information assets of the entity to ensure appropriate control design.
- iv) Clearly defining the roles and responsibilities including accountability for decision making within the entity for managing cyber risk, including in emergencies and crisis.
- v) Maintaining comprehensive cyber risk registers: Key cybersecurity risks should be regularly identified and assessed. Risk identification should be forward-looking and include security incident handling.
- vi) Ensuring implementation of the cyber and information risk management strategy.
- vii) Safeguarding the confidentiality, integrity, and availability of information.
- viii) Quantifying the potential impact by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.
- ix) Reporting all enterprise risks consistently and comprehensively to the board to enable the comparison of all risks equally in ensuring that they are prioritised correctly.

7.4. Risk Controls

- (a) Entities shall be required to:-
 - i. maintain a comprehensive incidence response plan;
 - ii. observe a strict patch management lifecycle;
 - iii. implement perimeter defence to protect networks from attacks executed through the internet, for example, firewalls;
 - iv. isolate sensitive company data from personal data;
 - v. train employees on cybersecurity basics to protect organizations from disastrous attacks;
 - vi. implement power user authentications for the authentication of users;

- vii. observe strict access controls; and
- viii. antivirus solutions in use should consist of available security controls.

8. MONITORING

- 8.1. The registered entities shall establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.
- 8.2. Registered entities must:
 - (a) Protect network (hardware, firmware, and software components) integrity including control of information flow, boundary protection, and network segregation if needed.
 - (b) Recognise signs of a potential cyber incident, or detect that an actual breach has taken place.
 - (c) Monitor relevant internal and external activities and events, in order to detect vulnerabilities through a combination of signature monitoring for known vulnerabilities and behaviorally-based detection mechanisms. Detection capabilities should also address misuse of access by third-party service providers, policyholders, potential insider threats, and other advanced threat activity through a strong cyber threat intelligence programme.
 - (d) Manage the identities and credentials for physical, logical, and remote access to information assets, based on principles of least privilege and separation of duties.
 - (e) Consider placing an effective intrusion detection capability which may include :
 - A. data loss/leaks prevention and detection;
 - B. the recording and documentation of audit logs;
 - C. event data aggregation, correlation, analysis and communication; and
 - D. network, personnel, and external dependency activity monitoring.

- (f) Employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process.
- (g) Rigorously test all elements of cybersecurity framework to determine their overall effectiveness before being applied within an entity, and regularly thereafter. Test results should be communicated within the organization and be used to support the ongoing improvement of the entity's cybersecurity. Proper procedures should be put in place to ensure that the board and senior management are appropriately involved and informed of test results.
- (h) Regulated entities should consider using certified testing methodologies and practices available.

9. RESPONSE AND RECOVERY

9.1. Response

- 9.1.1. Regulated entities shall respond promptly to cyber-attacks, taking into consideration the severity of the attack, curtailing its effects, issuing appropriate notifications to stakeholders, and coordinating and implementing responses that allow them to return to normal operations.
- 9.1.2. As part of response measures entities shall:
 - (a) Implement incident response policies and other controls to facilitate effective incident response. The controls should address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders.
 - (b) Upon detection of a cybersecurity incident (or an attempt), perform a thorough investigation to determine its nature and extent as well as the damage inflicted.
 - (c) Resume critical operations as soon as is safely possible after a cybersecurity incident. Analyse critical functions, transactions, and interdependencies to prioritize resumption and recovery actions while remediation efforts continue.

- (d) Consider implementing system and process design and controls for critical functions and operations to support incident response activities to the extent possible; and
- (e) Have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative processes.

9.2 Recovery

- (a) With regards to recovery, regulated institutions shall:-
 - (i) Have in place validated plans and procedures to recover from a cybersecurity incident. Cyber incident recovery arrangements should be designed in a way that enables entities to resume operations safely with a minimum of disruptions to policyholders, fund members and business operations.
 - (ii) Design and test their systems and processes to enable timely recovery of accurate data following a breach.
 - (iii) In the event of a cyber incident where system and process are interconnected with third-party service providers, an entity shall work with these third parties to resume operations safely.
 - (iv) Have formal plans for communicating with policyholders, internal and external stakeholders likely to sustain harm due to a major cybersecurity incident.

10. TRAINING AND AWARENESS

- 10.1. Considering that cyber risks and vulnerabilities change rapidly, and so does the best practices and technical standards for addressing them, regulated entities shall:
 - (a) Provide adequate training to all system users on the subject of cybersecurity awareness and the latest developments in cybersecurity, taking into account the type and level of cyber risks they may face.
 - (b) Promote the professional competence and capacity of their staff, especially those responsible for cybersecurity and systems.

- (c) Establish a process to gather and analyse relevant cyber risk information and participate in information sharing groups, like information sharing intelligence platform, for timely information sharing to allow spontaneous and appropriate precautionary measures to be taken in combating cyber-attacks and other forms of cyber risks, both locally and internationally.

11. REPORTING

- 11.1. Every regulated entity shall be required to review and submit their cybersecurity strategy, policy, and frameworks on yearly basis.
- 11.2. The entities should notify the Commission and relevant internal and external stakeholders, within 24 hours of any cybersecurity incident(s) that could have a significant and adverse impact on the entity's ability to provide adequate services to its customers, its reputation, or financial condition.
- 11.3. Every quarter, entities shall provide the Commission with a report concerning the occurrence and handling of cybersecurity incidents.

12. COMPLIANCE

- 12.1. The Commission shall monitor and enforce compliance with the provisions of this Framework.

End of Framework
