

GOVERNMENT NOTICE No. 394 published on 3/08/2018

SOCIAL SECURITY (REGULATORY AUTHORITY) ACT,
(CAP. 135)

—————
GUIDELINES
—————

(Made under section 5(1)(c))
—————

THE SOCIAL SECURITY SCHEMES (RISK MANAGEMENT) GUIDELINES, 2018

ARRANGEMENT OF GUIDELINES

<i>Paragraph</i>	<i>Title</i>
PART I PRELIMINARY PROVISIONS	
1.	Citation.
2.	Application.
3.	Interpretation.
4.	Objectives.
PART II RISK MANAGEMENT PLAN AND PROCESSES	
5.	Risk management plan.
6.	Risk management processes.
7.	Risk management framework.
8.	Set up of risk management.
9.	Function of risk management.
PART III INDEPENDENT REVIEW	
10.	Independent review.
11.	Independent reviewer qualifications.
12.	Reviewer assessment.

PART IV
RISK GOVERNANCE

- 13. Risk governance.
- 14. Review of policies relating to risk.
- 15. New investments and strategic activities.

PART V
BUSINESS CONTINUITY ON RISK MANAGEMENT

- 16. Business continuity policies and practices.
- 17. Minimum requirements for data availability.
- 18. Integration of risk management.
- 19. Contingency planning.

PART VI
GENERAL PROVISIONS

- 20. Sanctions.
- 21. Dis-application of Guidelines and savings.

GOVERNMENT NOTICE No. 394 published on 3/08/2018

SOCIAL SECURITY (REGULATORY AUTHORITY) ACT
(CAP. 135)

GUIDELINES

(Made under section 5(1)(c))

THE SOCIAL SECURITY SCHEMES (RISK MANAGEMENT) GUIDELINES, 2018

PART I
PRELIMINARY PROVISIONS

Citation	1. These Guidelines may be cited as the Social Security Schemes (Risk Management) Guidelines, 2018.
Application	2. These Guidelines shall apply to all Schemes operating in Tanzania Mainland.
Interpretation	3. In these Guidelines, unless the context otherwise requires-
Cap. 135	“Act” means the Social Security (Regulatory Authority) Act; “Authority” means the Social Security Regulatory Authority established under section 4 of the Act; “Board” means the Board of Trustees of a Scheme established by the scheme’s law or Trust Deeds; “business continuity” means a set of planning, preparatory and related activities which are intended to ensure that schemes’ critical business functions continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period; “control” means any measure or action that mitigate risks, and may include any policy, procedure, practice, process, technology, technique, method or device that modifies or manages risk; “monitoring” means to determine the current status and to assess

- whether or not required or expected performance levels are actually being achieved;
- “risk” means the possibility of an event occurring that will have a negative impact to the achievement of objectives and may be measured in terms of impact;
- “risk analysis” means the systematic use of available information to determine the likelihood of specified events occurring and magnitude of their consequences;
- “risk assessment” means a process that is, in turn, made up of three process namely risk identification, risk analysis, and risk evaluation;
- “risk champion” means a person designated as such in a department or unit who is responsible for ensuring that the risk register of the department or unit is at all time up to date;
- “risk identification” means process that involves finding, recognizing and describing the risks that may affect the achievement of an organization’s objectives;
- “risk management” means a process of identifying, assessing, managing and controlling potential events or situations to provide reasonable assurance regarding the achievement of scheme’s objectives;
- “risk management framework” means a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the scheme’s organization;
- “risk management plan” means a document prepared by a scheme pursuant to these Guidelines to show how risk management programs of the scheme are implemented over a given period of time;
- “risk management policy” means a statement that defines a general commitment, direction or intention;
- “risk owner” means a senior official responsible for the area that the risk will have most impact or that has been assigned the responsibility for the risk by the scheme;
- “risk treatment” means a process of selection and implementation of measures to modify risk which includes selecting and implementing one or more treatment options;
- “scheme” means the social security scheme and includes mandatory and supplementary schemes.

Objectives of Guidelines

- 4.** The objectives of these Guidelines shall be-
- (a) to enhance risk management practices among schemes; and
 - (b) to provide insights on steps to be followed by schemes when developing and implementing customized risk management frameworks.

PART II
RISK MANAGEMENT PLAN AND PROCESSES

Risk management plan

- 5.-(1)** A scheme shall have a comprehensive risk management plan tailored to its needs and circumstances under which it operates.
- (2) The scheme shall, at least once in every financial year, review its risk management plan.

Risk management process

- 6.** The risk management process shall consist of five key steps as follows-
- (a) risk identification;
 - (b) risk measurement;
 - (c) risk control;
 - (d) risk monitoring; and
 - (e) risk reporting.

Risk management framework

- 7.-(1)** A scheme shall put in place an effective risk management framework which shall adequately capture and manage all risks which the scheme is exposed to and have flexibility to accommodate any change in business activities.
- (2) Key elements of an effective risk management framework shall be-
- (a) active Board and Senior Management oversight;
 - (b) adequate policies procedures and limits;
 - (c) adequate risk measurement, monitoring and management information systems and comprehensive internal control.

Set up of risk management

- 8.** (1) A scheme shall put in place a setup that supervises overall risk management and shall be responsible for overseeing management of risks inherent in its operations.
- (2) The setup of risk management shall be in the following form-
- (a) Risk Management Board Committee;

- (b) Risk Management Committee;
- (c) risk owner;
- (d) Chief Risk Officer or a senior post; and
- (e) risk champions of each department depending on the size and complexity of the scheme.

Functions of risk management

9. The management shall ensure that effective processes are in place for-

- (a) identifying current and future emerging risks;
- (b) developing risk assessment and measurement systems;
- (c) establishing policies, practices and other control mechanisms to manage risks;
- (d) developing risk tolerance limits for senior management and Board approval;
- (e) monitoring positions against approved risk tolerance limits; and
- (f) reporting results of risk monitoring to senior management and the Board.

(2) Notwithstanding sub paragraph (1) risk management shall not be restricted to persons responsible for overall risk management function.

PART III
INDEPENDENT REVIEW

Independent review

10.-(1) A scheme shall have an independent risk reviewer who shall be responsible for reviewing the effectiveness of and adherence to the scheme's risk management policy and practice.

(2) The independent risk reviewer under paragraph (1) may also be conducted by-

- (a) internal auditors;
- (b) external auditors;
- (c) any other person who is independent from risk taking units.

(2) The independent risk reviewer shall report to the Director General and to the designated Risk Management Committee of the Board.

(3) Audit Committee shall report to the Board of Trustee on the results of the risk review.

Independent reviewer

11.-(1) An independent risk reviewer of the scheme shall have at least a bachelor degree in actuarial science, statistics,

- qualifications
- economics, banking, insurance, law, social protection, commerce or accounting, auditing and risk management from a recognized university.
- (2) A person shall not qualify to be appointed as an independent risk reviewer unless such person has the following qualifications-
- (a) at least five years' experience in risk related fields and has demonstrate sufficient ability to identify new risks facing the schemes;
 - (b) sufficient experience in the rollout of a risk management methodology;
 - (c) sufficient experience in strategic business planning; and
 - (d) Sufficient experience in tools and techniques for evaluation, presentation and maintenance of strategic and operational risks workshops and interviews.
- (3) Without prejudice to subparagraph (1), an independent risk reviewer shall possess sufficient knowledge and understanding of-
- (a) good governance, internal control systems and must demonstrate ability to monitor risk management activities or programmes and implementation thereof;
 - (b) internal audit and assurance practices;
 - (c) organisation risk management concepts, frameworks and methods; and
 - (d) risk finance and risk control concepts.

Reviewer
assessment

- 12.**-(1) A scheme shall, when outsourcing risk management, ensure an independent risk reviewer has sufficient expertise.
- (2) The independent risk reviewer shall, among other things, assess whether-
- (a) the scheme risk management system is appropriate to its nature and establishment of the scheme and as well as its activities;
 - (b) the scheme has an independent risk management function;
 - (c) the Board and senior management of the scheme are actively involved in the risk management process;
 - (d) policies, controls and procedures concerning risk management are well documented and complied at all levels;

- (e) assumptions made in risk measurement system are valid and well documented, data accurately processed and data aggregation is proper and reliable; and
- (f) the scheme has adequate staffing to conduct a sound risk management process.

(2) Notwithstanding any other provision under these Guidelines, the Authority, where necessary and for purposes of ensuring effectiveness of, and adherence to, the scheme's risk management policies and practices, may conduct independent risk review.

PART IV
RISK GOVERNANCE

Risk governance

13. A scheme's risk management shall have mechanisms for evaluating, monitoring and limiting risk for purpose of good governance on the following areas-

- (a) liquidity risk which includes funds to cover benefits payable in the year;
- (b) operational risk which includes systems compliance with contribution obligations, record keeping, staffing and transactions;
- (c) liability risk which includes contingent liability of the scheme;
- (d) economic risk which includes cyclical variations in employment levels, wage and price inflation;
- (e) investment risk which includes asset values and returns;
- (f) political risk on issues which have impacts for the social security schemes;
- (g) catastrophe risk such as natural disasters and epidemics;
- (h) strategic risk; and
- (i) reputational risk.

Review of policies relating to risk

14. Without prejudice to the provisions in the respective scheme law the Board shall review -

- (a) at least annually, all programmes relating to various types of risks and determine the ceiling of exposure permitted in the various risks and activity segments in accordance with the relevant regulations and guidelines;

- (b) and approve organisational arrangements for managing and controlling the scheme's overall exposure to various risks in line with the relevant Guidelines issued by the Authority.

Risk assessment in new investments

15.- (1) Chief Risk Officer shall inform the Board on new investments and strategic activities of the scheme.

(2) The information under sub-paragraph (1) shall include the following -

- (a) risks involved in that new investment;
- (b) mechanisms the scheme will use for managing and controlling of risks emanating from such investment;
- (c) the quantitative restrictions required in connection with the risks embodied in the investment;

PART V

BUSINESS CONTINUITY ON RISK MANAGEMENT

Business continuity and practices

16. A scheme shall formulate and implement written business continuity policies and practices.

Minimum requirements for data availability

17. Notwithstanding the Social Security Scheme (Data Management) Guidelines, 2018, the Board of a scheme shall ensure that at least -

- (a) there is an information technology disaster recovery plan for electronic data in place;
- (b) backup of all information related to membership information, contributions, benefits paid and investments made, is done within seventy two hours of any change to the data;
- (c) one copy of the most current backup of the scheme member's data is kept at a location that is not the main operating premises of the scheme;
- (d) the location is seven kilometers from the main operating premises of the scheme;
- (e) a record of individual member's complete personal details and last contribution received is in backup;
- (f) once a year, records of the members held by the scheme are availed to members or employers for reconciliation and updating upon request.

Integration of risk management

18. The scheme shall have a structure in place to monitor

risk interrelationships across the scheme.

Contingency
planning

19.-(1) A scheme shall have a mechanism to identify stress situations ahead of time and plans to deal with such unusual situations in a timely and effective manner.

(2) The plans shall be tested as to the appropriateness of the following-

- (a) responses;
- (b) escalation and communication channels; and
- (c) the impact on other parts of the scheme.

**PART VI
GENERAL PROVISIONS**

Sanctions

20.-(1) Any Scheme which contravenes the provisions of these Guidelines commits an act of unsafe or unsound conduct as provided in the Act, and such act shall be punishable in the manner provided in the Act.

(2) Notwithstanding the penalty imposed under sub paragraph (1), the Authority shall have the powers to-

- (a) direct the Scheme to comply with these Guidelines;
- (b) propose disqualification of the Board of Trustees of Schemes and Management of the Schemes to the respective appointing authority;
- (c) take any other necessary measures it considers appropriate for the better implementation of these Guidelines.

Dis-application of
Guidelines and
savings

21.-(1) The Social Security Schemes (Risk Management) Guidelines, 2016 issued prior to the coming into effect of these Guidelines are hereby disappplied.

(2) Notwithstanding sub paragraph (1), anything done, action, claim or directive made pursuant to the Social Security Schemes (Risk Management) Guidelines, 2016 shall continue to have effect as if were made, issued or prepared under these Guidelines.

Dodoma
....., 2018

IRENE C. ISAKA
Director General