Finnet

Building a Better Tomorrow, Today

TOPIC : ENTERPRISE RISK MANAGEMENT FOR PENSION FUNDS

RISK MANAGEMENT, STRATEGY AND POLICY FORMULATION PROGRAMME FOR PENSION FUNDS

DATE 8TH – 12TH DECEMBER 2025

VENUE – PRIDE INN PARADISE, MOMBASA

GOVERNANCE . TRAINING . EMPLOYEE BENEFITS . TECHNOLOGY

Definition of Enterprise Risk Management (ERM)

- ERM is a process, embedded in an organization's strategy setting to identify and manage risk to be within approved risk appetite, so as to provide reasonable assurance in attaining organization goals.

Definition of Enterprise Risk Management (ERM)

- Risk Management is a discipline at the core of every institution and encompasses all the activities that affect its risk profile.
- Risk management as commonly perceived does not mean minimizing risk; rather the goal of risk management is to optimize risk-reward trade-off.
- This can be achieved through putting in place an effective risk management framework which can adequately capture and manage all risks an institution is exposed to.
- Risk Management entails four key processes: Identification, Assessment, Control and Monitoring.

Definition of Enterprise Risk Management (ERM)

- **Risk Identification:** In order to manage risks, an institution must identify existing risks or risks that may arise from both existing and new business initiatives for example, risks inherent in lending activity include **credit, liquidity, interest rate and operational risks**.
- Risk identification should be a continuing process, and should occur at both the transaction and portfolio level.

Definition of Enterprise Risk Management (ERM)

- **Risk Measurement:** Once risks have been identified, they should be measured in order to determine their impact on the institution's profitability and capital.
- This can be done using various techniques ranging from simple to sophisticated models.
- Accurate and timely measurement of risk is essential to effective risk management systems.
- An institution that does not have a risk measurement system has limited ability to control or monitor risk levels.
- An institution should periodically test to make sure that the measurement tools it uses are accurate.
- Good risk measurement systems assess the risks of both individual transactions and portfolios.

Definition of Enterprise Risk Management (ERM)

- **Risk Control:** After measuring risk, an institution should establish and communicate risk limits through policies, standards, and procedures that define responsibility and authority.
- Institutions may also apply various mitigating tools in minimizing exposure to various risks.
- Institutions should have a process to authorize exceptions or changes to risk limits when warranted.

Definition of Enterprise Risk Management (ERM)

- **Risk Monitoring:** Institutions should put in place an effective management information system (MIS) to monitor risk levels and facilitate timely review of risk positions and exceptions.
- Monitoring reports should be frequent, timely, accurate, and informative and should be distributed to appropriate individuals to ensure action, when needed.

Risk Management Framework

- A risk management framework encompasses the scope of risks to be managed, the process/systems and procedures to manage those risks and the roles and responsibilities of individuals involved in risk management.
- The framework should be comprehensive enough to capture all risks an institution is exposed to and have flexibility to accommodate any change in business activities.

Risk Management Framework

- Key elements of an effective risk management framework are:
  - Active board and senior management oversight;
  - Adequate policies, procedures and limits;
  - Adequate risk measurement, monitoring and management information systems; and
  - Comprehensive internal controls.

Risk Management Elements

- **Risk Governance** – institutional risk management framework, risk culture
- **Risk Assessment** – likelihood & impact if risk occurs
- **Risk Quantification & Aggregation** – risk modelling
- **Risk Monitoring & Reporting** – dashboards
- **Risk & Control Optimization** – upside of risks

Risk Assessment

Risk funnel

Inherent risks

Risk mitigation/controls

Residual risks Current risks

Risk Quantification & Aggregation

- Undertaking “root-cause” analysis
- Linking key risk indicators (KRIs) to relevant risk appetite thresholds
- Updating risk registers with KRIs per process
- Risk modelling, economic/solvency capital vs own funds

Risk Monitoring & Reporting

- Performance of KRIs against set risk appetite thresholds
- Reported risk incidents (Loss events/incident management) – loss data framework
- Management reporting to the board on existing and emerging risks (on quarterly basis)

Risk & Control Optimization

- Identification of improvements for top risks
- Proactive as opposed to reactive risk responses
- Risk Control self-assessments (RCSAs) on effectiveness of risk mitigation/controls
- Evidence of risk-informed decisions i.e. undertaking risk assessments before effecting major decisions

Emerging trends in Risk Management

- **Increased emphasis on emerging risks** – sophistication in evaluating "unknown" risks (‘"black swans", "Zero-day attacks") via risk modelling (stress testing and scenario analysis)
- **Increased and rapidly changing regulatory compliance requirements e.g. data privacy & location laws** – GDPR in Eurozone and Data Protection Act in Kenya (cost of compliance)
- **Infusion of data analytics, technology and strategy**(appetite) into risk management (including cloud risk and compliance concerns)

Emerging Risks

- Risks (existing or developing) that are difficult to predict or quantify and may have high loss potential due to their high uncertainty e.g.
  - **Inherent risks to 4th Industrial Revolution (4IRs) – block chain, AI, big data & IoT, 3D printing, robotics, etc.**
  - **Cyber security related risks- CIA (confidentiality, integrity and availability)- creating cyber resilience, adequacy of benefit realization planning (BRP), etc.**
  - **Unknown or unpredictable events – e.g. zero-day attacks and & "black swan" events e.g. Covid-19 pandemic, global scale cyber attack, etc.**
  - **Laws and regulations on cyberspace – GDPR, Data Protection Act (balancing privacy, security and ROI on IT investments). Supervision & regulation on cyber risk at nascent stage in most jurisdictions**

Finnet
Building a Better Tomorrow, Today

Enterprise Risk Management Today

Risk governance operating model design : 3LOD
Key principles

Many financial institutions have adopted the 3LOD principles in relation to the design of their risk governance operating models. Whilst the Solvency II requirements are consistent with these principles some modifications are likely to be required.

Corporate Governance Code 2013 (effective 1/1/2015)

- **Policy**
  - Risk Appetite Statement

- **Implementation**
  - Chief Risk Officer

- **Oversight**
  - Risk Committee

Policy - Risk Appetite Statement

- Risk Appetite statement must "address separately the short-, medium- and long-term horizons"
- "The Board is required to understand the risks to which the institution is exposed…"
- "The appetite shall be expressed in qualitative terms and also include quantitative metrics…"

What might a Risk Appetite Statement look like?

- Put it in context with the entity's goals
- A brief overview: "*The Risk Appetite is the level of risk required to achieve objectives A, B and C*"
- List risk categories (6-12 perhaps)
- Solvency II uses "1 in 200-year event" approach
- Tabulate, e.g.:

Risk Type	Scenario	Appetite
Equity	50% fall in markets	A-L ratio worsens 10%

The Chief Risk Officer

- "The CRO shall be responsible for ensuring that the institution has effective process in place…and manage risks to which the institution is or might be exposed."
- "CRO shall have relevant expertise, qualifications and background…
  - seniority and independence"
- "The CRO shall promote sound and effective risk management…"
- The CRO shall provide "…comprehensive and timely information on…material risks which enables the board to understand the overall risk profile of the institution."

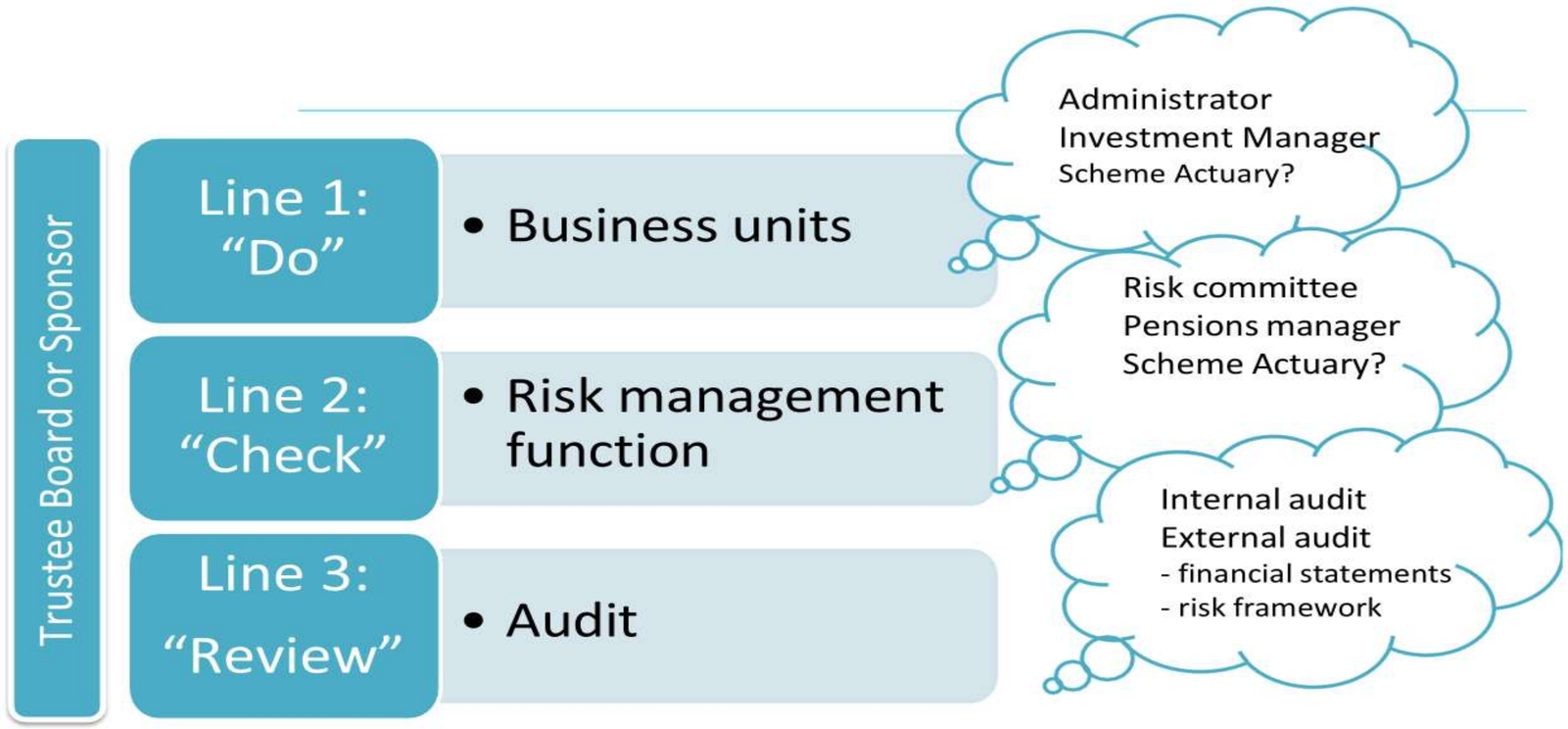
The Risk Committee

- "The number of members of a risk committee shall be sufficient to handle the nature, scale and complexity of the business…"
- "The Chairman of the Risk Committee shall be a non- executive director"
- The CRO and Risk Committee must, jointly, ensure that
- the "risk management system… is effective and proportionate to the nature, scale and complexity of the risks inherent in the business"

Finnet
Building a Better Tomorrow, Today

PROPOSED RISK MANAGEMENT FRAMEWORK

High Level Model: 3LoD

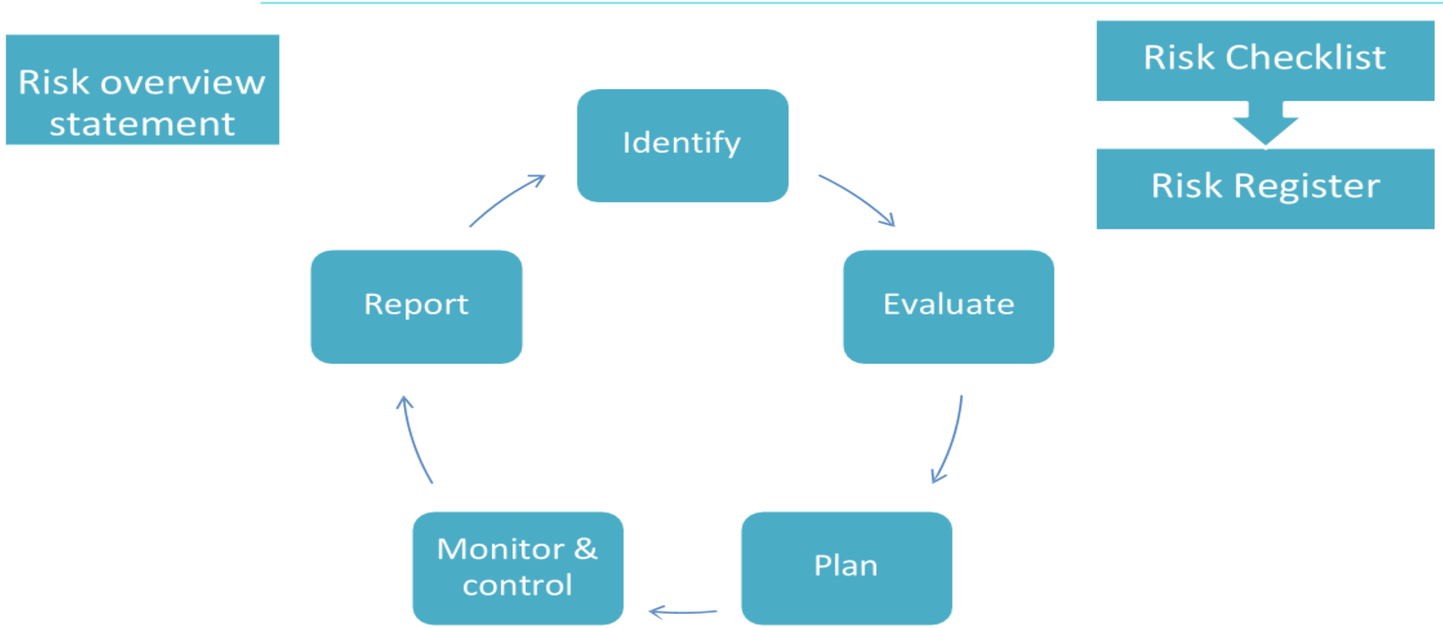


High Level Model Roles And Responsibilities

- No definitive answer as to exact structure of model and who fits in to which line
  - Depends on nature, size and complexity of the scheme and sponsor

- Key concepts for all schemes
  - Segregation of responsibilities
  - Effective challenge between the lines

Suggested Risk Management Framework



Documentation

Risk Overview Statement

- **Statement of trustees' appetite / attitude to risk - a "mission statement"**
- **Structural elements**
  - Trust Deed and Rules, balance of powers summary, service agreements etc.
- **Governance approach**
  - Trustee board membership, subcommittees, frequency and conduct of meetings, decision making processes, register of interests etc.
- **Policy suite**
  - SIPP, funding plan, conflicts of interest, dispute resolution, data protection etc.
- Sample content (base line of minimum requirements / good practice/ ideal approach) drafted and will be available on website.

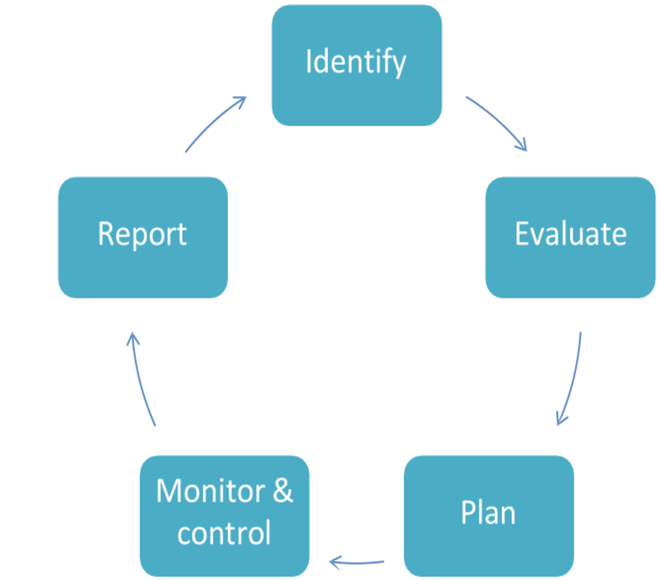
Pension Protection Fund – risk appetite statement

- "In general, the Board has a *cautious risk appetite with respect to all risk categories apart from investment operations where it is even more risk averse*".
- "We will *take risks that have been carefully considered and where controls have been implemented to reduce the likelihood of a risk materializing or the impact if one did materialize*".
- "Where commercially viable, we would expect *financial risks to be hedged* through appropriate instruments or insurance".
- *"Risks will be monitored by the use of key risk indicators as agreed by the Executive team* through the Asset and Liability Committee and the Risk Management Committee as described in our risk management policy".

Risk Checklist and Risk Register

- **Risk checklist**
  - Generic list of all potential risk to a scheme
  - Facilitates discussion on the risks particular to the scheme
- **Risk register**
  - Statement of risks particular to the scheme
  - Record of outcome of various stages of risk management system
    - ✓ Risks identified in most recent review (**identify**)
    - ✓ Ranked / prioritized according to exposure (**evaluate**)
    - ✓ Agreed mitigation / management approach (**plan**)
    - ✓ Reporting responsibilities (**report**)
  - Reviewed and refreshed at agree intervals (**Monitor**)
  - Sample documents prepared and will be available on the website

Risk Management Cycle



Risk Management Cycle: Identify

- Risk grouped into the following categories
  - Scheme management
  - Funding and Solvency
  - Investment
  - Operational
  - Legislative
  - Sponsor covenant

Risk Management Cycle: Evaluate

- Evaluate risk by:
  - Likelihood
  - Impact
- **Non-financial risks** are likely to require qualitative measure of risk
- **Financial risks** may allow some quantitative measures
  - VaR
  - Scenario / sensitivity
- Modelling and consideration proportionate to nature and scale of risk
- Consider the correlations between risks

Risk Management Cycle: Plan

- Important to remember not the aim to eliminate all risks
- Rather aim is to understand the risks involved and
  - **Remove** risk
  - **Reduce** likelihood or/and impact risk to an acceptable level
  - **Transfer** (some or all of) the risk to other parties
  - **Accept or exploit** risk
- Note decisions in risk register
- Assign responsibility for each risk

Risk Management Cycle: Monitor

- Review of **risk checklist** and **risk register**
  - For effectiveness of risk mitigation processes previously agreed
    - ✓ Performance of individuals and entities involved in scheme operation
    - ✓ Examine areas where mitigation did not work as planned
    - ✓ Examine areas where agreed mitigation was not (fully) implemented
  - For new risks and relevance of risks previously included
  - Agree frequency of reviews
    - ✓ High level review annually
    - ✓ More formal review every three years (unless significant change in circumstances of scheme)
- Review **risk management framework**
  - Periodic external review

Risk Management Cycle: Report

- By third party providers to the trustees – in relation to delegated functions
  - Legislative compliance
  - Service levels
  - Risk incidents / issues
  - Emerging risks
- By trustees to members
  - Disclosure of risk appetite / attitude statement
  - For DB schemes – risk analysis in triennial valuation report
  - Should trustees perhaps report to members on their regular reviews of the scheme's risk register?
- By trustees to regulator?
  - How / when to evidence risk management?

Finnet
Building a Better Tomorrow, Today

THANK YOU

Talk to me!

0720272784 / 0748909546

AARON LUDENYO MUKHONGO

PhD; ICPAK; MKIM

ALUMO Management Consultants Ltd.

EMAIL: aaronmukhongo@alumo.co.ke

Finnet

Building a Better Tomorrow, Today

Daphton Court, Riverside Drive, Westlands
P.O.B ox 48179 -00100, GPO Nairobi, Kenya
Call: +254 719 560 656, +254 740 257 777, +254 11 1052230
Email: institute@finnettrust.com | info@finnettrust.com

www.finnettrust.com

Finnet Trust