EXECUTIVE SCHOOL OF
GOVERNANCE & MANAGEMENT

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT · MASTERCLASS

Scheme Governance Audit: Procedure & Strategy

Date: 28 October 2026 | Day Three | Facilitator: Sospeter Thiga

Governance | Training | Employee Benefits | Insurance

About the Facilitator



Sospeter Thiga

MBA | CPA | CISA | IRMCert | CRMA

Current Role
CPF Group Head of Risk & QA, DPO, MLRO

Experience
20 years in GRC & Auditing

Board Memberships
Utana Foundation, KiMAP, Tanari Trust, IRM EA (Co-Chair)

Skill-set & Passion
Trainer, Coach, GRC Expert, Author, Social Impact, Nature

OPENING THOUGHT

“Trust, but verify.”

Russian Proverb

Which controls in your scheme are verified — and which are simply trusted?

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Session Objectives & Agenda

- **Understand the scheme governance and assurance landscape**
- **Apply practical audit procedures to contributions, benefits and investments**
- **Design a risk-based audit strategy and plan**
- **Report findings and track actions to closure**

Run of Session

0–10 min **Governance & assurance landscape**

10–35 min **Audit types, lifecycle & procedures**

35–60 min **Case studies (group work)**

60–75 min **Strategy, reporting & follow-up**

75–90 min **Knowledge check & action plan**

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Why the Scheme Audit Matters

Stewardship of Member Assets

Members depend on trustees to safeguard long-term retirement savings.

Regulatory Compliance

Scheme must meet the Retirement Benefits Act, RBA regulations and its trust deed.

Trust & Transparency

Credible audited accounts and reports sustain confidence of members and sponsors.

Early Warning

Audit surfaces control failures, fraud and arrears before they become losses.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Scheme Governance: Who Does What

Oversight & Assurance

- Members & Sponsor
- Regulator (RBA)
- External Auditor
- Internal Audit & Risk/Audit Committee

Board of Trustees

Accountable for the scheme

Service Providers

- Scheme Administrator
- Custodian
- Fund Manager(s)
- Actuary

Three Lines of Assurance in a Scheme

Line	Who	Role	Scheme Example
1st line	Administrator, scheme management	Own and operate controls	Contribution posting, benefit processing
2nd line	Risk & compliance functions	Set policy, monitor and challenge	Risk register, compliance monitoring against RBA rules
3rd line	Internal audit	Independent assurance to the committee	Risk-based audit of contributions, benefits, investments
External	External auditor, actuary, RBA	Independent opinion and supervision	Annual audit, actuarial valuation, regulatory returns

Types of Scheme Audit



Financial Statement Audit

Opinion on fair presentation under IAS 26 and applicable ISAs.



Compliance Audit

Adherence to the Act, regulations, trust deed and rules.



Investment Audit

Limits, valuation, custody and policy adherence.



Contributions & Benefits

Completeness of contributions; accuracy of payments.



IT & Data Audit

Access, integrity, backup and data protection.



Governance Audit

Trustee oversight, conflicts, training and decision records.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

The Audit Lifecycle

Every stage produces evidence the Risk & Audit Committee can rely on.

1. PLAN

Plan

Scope, objectives, resources and timing agreed with the committee.

2. ASSESS

Assess Risk

Understand the process, identify risks and key controls.

3. TEST

Fieldwork

Test controls and transactions; gather evidence.

4. REPORT

Report

Communicate findings, ratings and agreed actions.

5. FOLLOW UP

Follow Up

Verify that actions are completed and sustained.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Building a Risk-Based Audit Strategy

Audit what could hurt members most — not what was audited last year.

Define universe

List all processes, providers and systems.

Rate risks

Score impact, likelihood and control strength.

Prioritise

Focus on highest residual risk and regulatory focus areas.

Resource & schedule

Match skills, days and timing to the scheme calendar.

Approve & monitor

Committee approves the plan and tracks delivery.

Audit Universe: Key Risks & Tests

Area	Key Risk	Typical Audit Test
Contributions	Under or late remittance	Reconcile payroll schedules to bank and member accounts; chase arrears
Benefit payments	Wrong or ghost payments	Verify claims to source documents and ID; recompute benefits
Investments	Loss, limit breach, wrong valuation	Test to IPS and RBA limits; confirm holdings with custodian
Member records	Inaccurate balances	Reconcile register to ledger; test interest crediting
Governance	Weak oversight, conflicts	Review minutes, conflicts register and trustee training
ICT & data	Data breach, system error	Test access, backups and Data Protection Act compliance

Audit Procedure: Contributions

Completeness test: are all deductions received and credited to members?

Obtain schedules

Payroll and sponsor remittance schedules per month.

Reconcile to bank

Match receipts to schedules; quantify differences.

Trace to members

Test posting to individual member accounts.

Test timeliness

Compare receipt dates with statutory due dates.

Report arrears

Escalate ageing arrears to trustees and committee.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Audit Procedure: Benefit Payments

Accuracy and validity test: right person, right amount, right authority.

Claim received

Select sample of claims across the period.

Verify identity

ID, bank details, life certificates, beneficiary forms.

Recompute

Re-perform benefit calculation against scheme rules.

Approve & pay

Check authorisation levels and segregation of duties.

Post & reconcile

Agree payment to bank and member ledger.

Investment Audit: What to Check

Key Controls to Test

- Investment Policy Statement approved and reviewed
- Limits monitored monthly against RBA guidelines
- Custodian confirmations agree to records
- Independent valuation of unlisted assets
- Conflicts and related-party checks documented

Red Flags

- Concentration in one counterparty or sector
- Illiquid assets with stale valuations
- Related-party transactions without approval
- Late or missing valuation reports
- Breaches noted but never escalated

Evidence & Sampling

Sufficient & Appropriate

Evidence must be relevant and reliable, in line with ISA 500.

Risk-Based Samples

Larger samples where risk is higher; consider ISA 530.

External Confirmations

Custodian, bank and fund manager confirmations beat internal reports.

Analytical Review

Trend and ratio analysis to spot unusual movements.

Fraud & Irregularity Red Flags

Unreconciled Contributions

Persistent "timing differences".

Ghost Pensioners

Duplicate bank accounts, no life certificates.

Bank Detail Changes

Unusual changes before payment runs.

Control Override

Management bypass of approvals.

Related-Party Deals

Investments with connected parties.

Missing Records

Documents "in transit" or unavailable.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Self-Reflection: Audit Procedures

Area	Score (1-5)	Reflection Question
Contributions	[ ]	Do we reconcile every payroll schedule to bank receipts and member accounts?
Benefit payments	[ ]	Are claims verified to source documents and independently approved?
Investments	[ ]	Do we confirm holdings and valuations with the custodian each year?
Evidence	[ ]	Do auditors rely on third-party evidence, not management explanations?
Fraud risk	[ ]	Do we run analytics for duplicate bank accounts and missing life certificates?

Score 1 = not in place · 3 = partly · 5 = fully embedded. Total under 15: priority gap | 15–20: developing | 21–25: strong

Case Study 1: The Contributions Gap

THE SCENARIO · GROUP EXERCISE (15 MIN)

Mti Mkubwa Staff Pension Scheme has 1,200 active members. Payroll deductions for the year exceed bank receipts by KES 38 million. The administrator calls it "timing differences". Trustees were last told of arrears 14 months ago.

Discussion Questions

1. Which audit procedures do you perform first?
2. What are the risks to members and trustees?
3. What is escalated to the committee and RBA, and when?
4. What strategy changes prevent recurrence?

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Case Study 2: The Ghost Pensioner

THE SCENARIO · GROUP EXERCISE (15 MIN)

A pension payroll pays 340 pensioners monthly. Analytics shows 9 pensioners sharing one bank account and 14 with no life certificate in 3 years. The administrator says certificates are "in transit".

Discussion Questions

1. What does the data tell you, and what do you test next?
2. Which controls failed?
3. How should the finding be rated and reported?
4. What should trustees do immediately?

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Trustees' Role & Audit Independence

Approve the Audit Charter

Defines mandate, authority and independence.

Appoint & Review Auditors

Assess quality, fees, rotation and independence.

Direct Access

Head of audit has unrestricted access to the committee chair.

Protect From Interference

Management cannot restrict scope, budget or reporting.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Writing Findings: The 5 Cs

Findings that explain cause and consequence get fixed — not just noted.

Condition

What we found — the facts.

Criteria

The standard, rule or policy expected.

Cause

Why it happened — the root cause.

Consequence

The risk or impact on the scheme and members.

Corrective Action

Agreed action, owner and due date.

Rating Findings & Agreeing Actions

Rating	Meaning	Escalation	Typical Timeline
High	Material loss, fraud or regulatory breach	Immediately to committee chair and Board	**Within 30 days**
Medium	Significant control weakness	To committee at next meeting	**Within 90 days**
Low	Minor improvement opportunity	Reported to management; summarised to committee	**Within 180 days**

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Follow-Up: Closing the Loop

No action is closed on assertion — only on evidence.

Log action

Record every agreed action in one register.

Assign owner

Named owner and a realistic due date.

Track status

Monthly status updates from owners.

Verify evidence

Audit confirms the fix works — not just claims.

Report to committee

Ageing and overdue actions reported each meeting.

Self-Reflection: Strategy & Follow-Up

Area	Score (1-5)	Reflection Question
Audit universe	[ ]	Is there a documented scheme audit universe with risk ratings?
Risk-based plan	[ ]	Does the plan target the highest residual risks and carry committee approval?
Independence	[ ]	Does internal audit report functionally to the committee chair?
Reporting	[ ]	Do findings state cause, consequence, owner and due date?
Follow-up	[ ]	Are overdue High actions escalated and closed on evidence?

Score 1 = not in place · 3 = partly · 5 = fully embedded. Total under 15: priority gap | 15–20: developing | 21–25: strong

Knowledge Check: Q1 of 5

Which line of assurance is independent of management and reports to the committee?

A First line — the administrator

B Internal audit

C Sponsor's finance team

D Fund manager

Knowledge Check: Q2 of 5

What is the best first step in building a risk-based audit plan?

A Repeat last year's plan

B Wait for an RBA directive

C Define the audit universe and rate the risks

D Audit the largest service provider

Knowledge Check: Q3 of 5

Payroll deductions exceed bank receipts. What do you do?

A Reconcile schedules to bank and member accounts, and quantify arrears

B Accept the explanation

C Reduce the sample size

D Exclude it from scope

Knowledge Check: Q4 of 5

Which "C" of a finding explains WHY the control failed?

A Condition

B Criteria

C Consequence

D Cause

Knowledge Check: Q5 of 5

A High-rated finding is overdue. What should happen?

A It is closed quietly

B It is moved to next year's plan

C It is downgraded to Medium

D It is escalated to the committee

Knowledge Check: Answer Key

Q	Answer	Rationale
1	B	Internal audit is the third line: independent of management, with a direct reporting line to the committee.
2	C	Risk ratings of the audit universe drive prioritisation.
3	A	Reconcile and quantify first; assertions are not evidence.
4	D	Cause is the root cause; it drives corrective action.
5	D	Overdue High findings must be escalated to the committee and Board.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Key Takeaways & Next Steps

Risk-Based, Not Routine

Plan audits around what could hurt members most.

Evidence Over Assertion

Reconcile, confirm and trace — don't rely on explanations.

Report With the 5 Cs

Cause and consequence turn findings into action.

Close the Loop

Track every action to verified closure and report to the committee.

EXECUTIVE SCHOOL OF
GOVERNANCE & MANAGEMENT

CLOSING THOUGHT

“There is nothing so useless as doing efficiently that which should not be done at all.”

Peter Drucker

What in your audit plan is being done efficiently but should not be done at all?

EXECUTIVE SCHOOL OF
GOVERNANCE & MANAGEMENT

Contacts

Sospeter Thiga

Trainer, Speaker & Consultant — Governance, Risk, Compliance & Financial Management

Crescent Business Centre (CBC), 5th Floor, Parklands, Nairobi

Email: sosthiga@gmail.com | info@esgm.co.ke

Phone: +254 722 676 484 | +254 719 560 656

www.esgm.co.ke

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Takeaway: IAS 26 — Retirement Benefit Plans

Statement of Net Assets

Plan assets less liabilities (other than promised benefits) give net assets available for benefits.

Changes in Net Assets

Contributions, investment income, benefits paid, expenses and transfers for the period.

Fair Value of Investments

Plan investments are carried at fair value; disclose the basis where fair value cannot be estimated.

Defined Contribution vs Benefit

DC: net assets and funding policy. DB: also actuarial present value of promised benefits and surplus or deficit.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Takeaway: ISA 500 — Audit Evidence

Sufficient & Appropriate

Sufficiency is quantity; appropriateness is quality — relevance and reliability.

External, independent, directly obtained and documentary evidence is more reliable than internal, indirect or oral evidence.

Procedures & Practice

Inspection, observation, confirmation, recalculation, reperformance, analytical procedures and inquiry. Inquiry alone is not enough.

In practice: confirm holdings with the custodian, trace contributions to bank statements, and do not rely solely on administrator explanations.

EXECUTIVE SCHOOL OF GOVERNANCE & MANAGEMENT

Takeaway: ISA 530 — Audit Sampling

Design for Purpose

Define objective and population; consider tolerable misstatement and expected errors.

Select Representatively

Random, systematic or monetary unit selection. Every item needs a chance of selection.

Know the Risks & Evaluate

Sampling risk vs non-sampling risk. Investigate deviations and project misstatements.

EXECUTIVE SCHOOL OF
GOVERNANCE & MANAGEMENT

Executive School of Governance & Management

Building a Better Tomorrow, Today

Crescent Business Centre (CBC), 5th Floor, Parklands, Nairobi
P.O. Box 48179-00100, GPO Nairobi, Kenya
Call: +254 719 560656, +254 740 257777, +254 11 1052230
Email: institute@esgm.co.ke | info@esgm.co.ke
Website: www.esgm.co.ke

Finnet Trust