Finnet
Building a Better Tomorrow, Today

PENSION STRATEGY FORMULATION EXCELLENCE & INNOVATION DRIVEN TRANSFORMATION

THE ROLE OF TECHNOLOGY & DATA MANAGEMENT IN PENSION GOVERNANCE

Finnet
Building a Better Tomorrow, Today

Key Elements of Corporate Governance

Accountability

Fairness

Transparency

Responsibility

CASE FOR CORPORATE GOVERNANCE

- Better access to resources
- Raw materials extracted and used in an environmentally friendly manner
- Effective, strategic decision-making
- Anti-corruption tools (ethics)
- If a listed company, commands a premium from investors (service providers demand)

CASE FOR CORPORATE GOVERNANCE

- Long term sustainability
- Operational/financial performance
- Improved oversight, monitoring & evaluation
- Human resource – skilled, healthy employees
- Access to Capital
- Succession planning

Finnet
Building a Better Tomorrow, Today

GOVERNANCE FAILURE

Understanding the Impact of Governance Failure

Inadequate oversight, ethical lapses, and weak internal controls directly undermine institutional trust, erode asset values, and imperil stakeholder security.

GOVERNANCE FAILURE

Consequences of Governance Failure

Regulatory penalties, severe financial losses, reputational damage, and loss of fiduciary integrity within pension schemes.

Finnet
Building a Better Tomorrow, Today

“The opportunity of a lifetime needs to be seized during the lifetime of the opportunity”

- Leonard Ravenhill -

Finnet
Building a Better Tomorrow, Today

CAN A ROBOT BE A CEO?

Finnet
Building a Better Tomorrow, Today

MINDSET FOR CHANGE

Adaptability

- **Embrace Change** – Be open to new ideas and technologies
- **Flexibility** – Adjust strategies and plans as needed
- **Resilience** – Bounce back from setbacks and failures

Continuous Learning

- **Stay Updated** – Keep abreast of industry trends and technological advancements
- **Curiosity** – Seek out new knowledge and experiences
- **Lifelong Learning** – Invest in personal and professional development

MINDSET FOR CHANGE

Decision Making

- **Risk Tolerance** – Be willing to take calculated risks
- **Data Driven Approach** – Make informed decisions based on evidence
- **Decisiveness** – Act promptly and confidently

Innovation

- **Creative Thinking** – Generate new ideas and solutions for people, process & systems e.g., "Think Fridays"
- **Experimentation** – Try out new approaches and learn from the results
- **Failure Tolerance** – View failures as opportunities for growth

MINDSET FOR CHANGE

5. Communication

- **Clear & Concise** – Communicate effectively with all stakeholders
- **Active Listening** – Pay attention to feedback concerns e.g. "In my shoes"
- **Transparency** – Be honest and open about challenges and success

6. Strategic Thinking

- **Visionary Leadership** – Develop clear and inspiring vision for the future
- **Alignment** – Ensure that digital initiatives align with overall organizational goals
- **Long-term Perspective** – Consider the long-term implications of decisions

Finnet
Building a Better Tomorrow, Today

WHY EMBRACE DIGITAL CHANGE?

Non-Linear

Small actions lead to disproportionate results. The unpredictability can create both risks and opportunities making it essential to understand the ripple effects of decisions.

Strategy

Stay agile by actively monitoring external and internal trends using scenario planning to prepare for multiple outcomes and building systems that allow for quick pivots to minimize risk and maximize opportunities.

Finnet
Building a Better Tomorrow, Today

WHY EMBRACE TECHNOLOGY?

Incomprehensible

Challenges too complex to fully understand and may be interconnected that resolving them may not be straightforward.

Strategy

Encourage collaboration by bringing together diverse perspectives and expertise.

Technology in Pension Schemes

Technology and data management transform pension governance by ensuring accuracy, transparency, and operational efficiency. Core elements include centralized data integration, automated compliance tracking, and secure digital access for stakeholders.

Use Cases Includes: 1. Operational Efficiency & Administration

- **Automated Workflows:** Software replaces manual record-keeping and benefit calculations, minimizing human error.
- **Single Source of Truth:** Capturing data once at the source—such as payroll uploads—eliminates duplicate entry and reconciles records instantly across administrators and custodians.
- **Faster Processing:** Digital platforms expedite benefit claims and status updates for members.

Technology in Pension Schemes

2. Transparency & Trust

- **Real-Time Dashboards:** Stakeholders and regulators view up-to-date funding levels, asset allocations, and performance metrics instantly.
- **Biometric Verification:** Facial recognition and fingerprints confirm beneficiary identities, eliminating "ghost pensioners" and fraud.
- **Member Portals:** Self-service tools give savers direct visibility into their accumulated retirement benefits.

Technology in Pension Schemes

3.0 Risk Management & Compliance & Analytics

- Artificial intelligence and machine learning flag compliance anomalies, contribution variances, and market risks early.
- **Audit Readiness:** Immutable digital logs create clear audit trails that satisfy statutory reporting requirements.

Technology in Pension Schemes

4.0 Investment of Scheme Funds

The emergence of virtual assets (cryptocurrencies) and Robo-advisors (software providing financial advice and portfolio management) offers new avenues for investment strategies.

5.0 Regulatory Technology (RegTech)

Technologies supporting Know-Your-Customer (KYC) compliance, machine-readable regulations, Robo-handbooks, and modelling / visualization tools can enhance regulatory processes and understanding.

Data Management in Pension Schemes

Effective data management ensures accurate benefit payouts, regulatory compliance, and fraud prevention within a pension scheme. Poor data quality leads to financial penalties, operational bottlenecks, and incorrect retirement calculations.

Core Components of Pension Data Management

- **Member Records:** Storing accurate personal details, employment histories, and contribution timelines.
- **Financial Integration:** Syncing real-time payroll data directly with investment custodian records.
- **Historical Tracking:** Preserving legacy scheme rules and past benefit accrual rates accurately.
- **Data Security:** Protecting sensitive personally identifiable information (PII) using robust encryption protocols.

Finnet
Building a Better Tomorrow, Today

Data Management in Pension Schemes

Critical Risks of Poor Data Management

- **Calculation Errors:** Incorrect data causes severe overpayments or underpayments to vulnerable retirees.
- **Regulatory Fines:** Financial regulators penalize schemes that fail to maintain clean data standards.
- **Increased Costs:** Manual clean-up operations drain administrative budgets and delay processing times.
- **Security Breaches:** Weak access controls leave highly sensitive member data vulnerable to cybercriminals.

Finnet
Building a Better Tomorrow, Today

Data Management Principles

- Data as a strategic Asset
- Data quality and integrity
- Unified Metadata Management
- Data accessibility and democratization
- Data security and privacy
- Data governance and stewardship
- Lifecycle data management
- Data integration and interoperability
- Master data management
- Data ethics and responsible use

TECHNOLOGY TRENDS SHAPING THE FUTURE

1. Blockchain: Ready for Business

The attractiveness of blockchain lies in the possibility of a new type of ledger – one that can be continuously updated and verified without the threat of being altered or corrupted.

a) Secure Record Keeping:

Blockchain offers an immutable and transparent ledger for storing legal documents, contracts and financial information.

- **Smart Contract:** Automated execution of legal agreements based on pre-defined conditions can streamline processes and reduce disputes.
- **Decentralized Processes:** Blockchain can enable decentralized procedures mechanisms, potentially bypassing traditional centralized approval systems.

TECHNOLOGY SHAPING THE FUTURE

Cyber Security: Real Defense

Data management and protection are hot topics in the financial sector. Schemes handle sensitive financial information which makes it a significant target for hackers and data breaches.

Cloud Goes Vertical

An important advantage of a cloud-based system is the continual updating of information, which allows to analyze data and make decisions based on cutting-edge information.

TECHNOLOGY SHAPING THE FUTURE

4. Artificial Intelligence (AI): Automating at Scale

As the application of AI to create self-learning systems continues to be integrated into accounting tasks, minute taking technological systems will take on repetitive and time-consuming jobs, leaving the analytical and managerial tasks to humans.

- **Predictive Analytics:** AI can analyze vast datasets to predict investment outcomes, identify potential biases, and optimize trading options.
- **Natural Language Processing:** This technology enables automated financial summarization, taking minutes, research and even profile clients and draft contracts.
- **Virtual Support:** While not a complete replacement for human support, AI can assist in preliminary clients' profile, routine decisions and even investment advice.

TECHNOLOGY SHAPING THE FUTURE

5. Big Data Analytics

Investing is significantly becoming more analytical, and technology will help push trading from reactionary and transactional to proactive and analytical.

6. Virtual and Augmented Reality (VR/AR)

- **a) Immersive Information Presentation:** VR can create realistic simulations of transaction outcomes, or other outcomes.
- **b) Remote Meetings:** AR can overlay digital information onto the physical world, enhancing the experience for remote participants.
- **c) Information Dissemination:** VR/AR can provide immersive training experiences to potential clients.

TECHNOLOGY SHAPING THE FUTURE

7. Facial Recognition & Biometrics

- **Identity Verification:** Biometric data can be used to verify the identity of clients.
- **Surveillance:** Facial recognition technology can aid in confirmation of legitimate clients.

8. Online Dispute Resolution (ODR)

- **a) Accessible Justice:** ODR platforms provide a convenient and cost-effective way to resolve disputes without the need for in-person court appearances.
- **b) Mediation and Arbitration:** AI-powered tools can assist in mediation and arbitration processes, offering neutral advice and facilitating settlements.

CATALYST FOR CHANGE - TECHNOLOGY

Digital transformation is re-shaping the way the scheme operates from onboarding of members, trustees, staff and service providers to offboarding. It is a shift towards leveraging technology to improve corporate governance.

Examples of Key Areas of Digital Transformation in the scheme:

Member Management

- **Centralized Databases** – Digitizing documents streamlines member management procedures
- **Workflow Automation** – Automating routine tasks such as scheduling consultations, sending information saves time and reduces errors
- **Electronic Filing** – Allowing members to lodge documents online reduces paperwork and improves transparency and accessibility

TECHNOLOGY: CATALYST FOR CHANGE

Client Support

- **Virtual Meetings** – Using video conferencing technology for some of the member engagement and board meetings reduces travel time and costs for the scheme
- **Digital Support Documents** – Presenting digital documents enhances scrutiny and efficiency
- **Transcription & Recording** – Automated transcription and recording systems improves accuracy and reduce the need for manual note-taking

Online Dispute Resolution

- **Mediation & Arbitration** – Providing online platforms for mediation and arbitration allows for more efficient and cost-effective dispute resolution
- **Negotiation Tools** – Offering tools for online negotiation can help parties reach settlements without resorting to court.

TECHNOLOGY: CATALYST FOR CHANGE

Research & Analysis

- **AI-Powered Research** – Using AI to analyze databases can help the scheme to find relevant information to support strategic outcomes more efficiently
- **Predictive Analytics** – Analyzing historical data to predict trading outcomes can assist in strategy and decision-making
- **Online Courses** – Cost effective means for the scheme to capacity build their staff and Trustees

5. Access to Information

- **a) Online Records** - Providing public access to records enhances transparency and accountability
- **b) Information Portals** – Offering online portals with relevant information and resources can empower stakeholders to understand and make informed decisions avoiding potential disputes from decisions made from ignorance

BENEFITS OF DIGITAL TRANSFORMATION

- **Improved Efficiency:** Automation of tasks and processes reduces workload and improves turnaround times
- **Enhanced Transparency:** Digital records and public access to information increase transparency and accountability
- **Increased Accessibility:** Member portal promotes accessibility to member in remote areas
- **Reduced Costs:** Digitization can reduce operational costs, such as paper consumption and travel expenses
- **Improved Decision Making:** Data-driven insights can inform better decision-making by the Trustees

> **"The digital race is not between the big and small but between the most agile and the ones resistant to change"**

CHALLENGES OF DIGITAL TRANSFORMATION

- **Digital Divide:** Ensuring equitable access to technology is crucial to prevent further marginalization of disadvantaged groups
- **Data Privacy & Security:** Protecting sensitive data and preventing cyber attacks is a top priority. Robert Kioko & Ferdinand Metropolis Star Lab fined Ksh.500,000/= for WhatsApp spam, privacy violations. (Sept 2024)
- **Resistance to Change:** Overcoming resistance to change from within can be challenging
- **Ethical Implications:** The use of AI and other emerging technologies raises ethical concerns related to bias and accountability

Finnet
Building a Better Tomorrow, Today

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Top Cyber Risks:

- **Ransomware:** Malicious software that locks or encrypts business files until a financial ransom is paid.
- **Phishing:** Fraudulent emails or messages designed to trick users into revealing passwords or sensitive data.
- **Distributed Denial of Service (DDoS):** Overwhelming a network with high traffic to shut down online services.
- **Cloud Misconfiguration:** Improperly secured cloud storage that accidentally exposes private databases to the public.
- **Supply Chain Exploits:** Hackers breaching a vulnerable third-party vendor to gain indirect access to a primary target

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Top Cyber Risks: Sources & Impact

Sources of Risk

- **External Threats:** Organized crime groups, nation-state actors, and compromised third-party vendors.
- **Internal Threats:** Human error, negligent employees clicking phishing links, or unapproved software use (shadow IT).

Business Impact

- **Tangible:** Direct financial loss, legal penalties, regulatory fines, and operational downtime.
- **Intangible:** Permanent damage to brand reputation and loss of customer trust.

Read AI Risks https://www.ibm.com/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them

Finnet
Building a Better Tomorrow, Today

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

The use of artificial intelligence continues to spread at a staggering speed. Companies worldwide have adopted and implemented AI, in solutions that are reshaping industries through improved efficiency, productivity and decision-making. However, many organisations have integrated AI into their business processes more quickly than they have updated security strategies and protocols.

Finnet
Building a Better Tomorrow, Today

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

To mitigate the cybersecurity risks in new AI solutions, organisations should review and update their existing cybersecurity programme to safeguard data and systems from inadvertent mistakes and malicious attempts.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Data governance

Use effective data governance to help ensure that data is properly classified, protected and managed throughout its life cycle is critical in the effective use of AI technologies. Implement secure data management and governance practices to help prevent model poisoning attacks, protect data security, maintain data hygiene and ensure accurate outputs. Good governance can include:

Finnet
Building a Better Tomorrow, Today

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

- **Policies and procedures:** Review and amend existing policies and procedures to define the necessary AI-specific security requirements, designate roles to oversee the AI operations and ensure implementation of the security guidelines.
- **Roles and responsibilities:** Establish policies with roles and responsibilities for governing data, along with defining requirements for documenting data provenance, handling, maintenance and disposal.
- **Data quality assessments:** Regular data quality assessments help identify and remove potentially malicious data from training datasets in a timely manner.
- **Data validation:** Data validation techniques like hashing can help ensure that training data is valid and consistent.
- **Identity and access management:** Identity and access management policies can help define who has access to data, with appropriate access controls to help prevent unauthorised modifications.
- **Acceptable data use:** Acceptable data use policies can outline what data can be used and how. Each data classification (such as public, internal, confidential or highly confidential) should include its uses and restrictions pertaining to AI technologies. Policies should also include procedures for users to follow if they find a restricted data type in an AI solution.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Threat-modelling

Conduct threat-modelling exercises to help identify potential security threats to AI systems and assess their impact. Some common threats to models include data breaches, unauthorised access to systems and data, adversarial attacks and AI model bias. When you model threats and impacts, you can identify a structured approach with proactive measures to mitigate risks. Consider the following activities as part of your threat modelling:

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

- **Criticality:** Document the business functions and objectives of each AI-driven solution, and how they relate to the criticality of your organisation's operations. This helps you to establish a baseline for criticality, making controls commensurate with the criticality of the AI application and determining the thoroughness of the threat model.

- **Connections:** Identify the AI platforms, solutions, components, technologies and hardware, including the data inputs, processing algorithms, and outputs. This will assist in identifying the logic, critical processing paths and core execution flow of the AI that will feed into the threat model and help edify the organisation on the AI application.

- **Boundaries:** Define system boundaries by creating a high-level architecture diagram, including components like data storage, processing, user access and communication channels. This will help you understand the AI application's data and activity footprint, threat actors and dependencies.

- **Data characteristics:** Define the flows, classifications and sensitivity for the data that the AI technology will use and the expected output. This will help determine the controls and restrictions that will apply to data flows, as you might need to pseudonymise, anonymise or prohibit certain types of data.

Finnet
Building a Better Tomorrow, Today

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

- **Threats:** Identify potential threats for your business and technologies, like data breaches, adversarial attacks and model manipulation.
- **Impacts:** Assess the potential impact of identified threats, and assign a risk level based on vulnerability, exploitability and potential damage.

- **Mitigation:** Develop and implement mitigation strategies and countermeasures to combat the identified threats, including technical measures like encryption, access controls or robustness testing, along with non-technical measures like employee training, policies or third-party audits.
- **Adaptation:** Review and update the threat model on an ongoing basis as new threats emerge or as the system evolves.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Access controls

To control access to your AI infrastructure, including your data and models, establish appropriate identity and access management policies with technical controls like authentication and authorisation mechanisms. To define the policies and controls you need to consider:

- Who should have access to what AI systems, data or functionality?
- How and when should access be re-evaluated, and by whom?
- What type of logging, reporting and alerts should be in place?
- If we use AI with access to real data that may contain personal data or other sensitive Information, what access controls do we need, especially as related to the data annotation process.

Reassess and update policies and technical controls periodically, to align with the evolving AI landscape and emerging threat types, ensuring that your security posture remains robust and adaptable.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Encryption and steganography

Encryption is a technique that can help protect the confidentiality and integrity of AI training data, source code and models. You might need to encrypt input data or training data, in-transit and at-rest, depending on the source. Encryption and version control can also help mitigate the risk of unauthorised changes to AI source code. Source code encryption is especially important when AI solutions can make decisions with potentially significant impact. To protect and track AI models or training data, you can use steganographic techniques such as:

- **Watermarking:** inserts a digital signature into a file, or the output of an AI solution, to identify when a proprietary AI is being used to generate an output.
- **Radioactive data:** makes a slight modification to a file, or training data, to identify when an organisation is using the training data. For instance, radioactive data can help you protect your public data against unauthorised use in the training of AI models

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

End-point security, or user and entity behaviour analytics

End points (like laptops, workstations and mobile devices) act as primary gateways for accessing and interacting with AI systems. Historically, they have been a principal attack vector for malicious actors seeking to exploit vulnerabilities. With AI-augmented attacks on the horizon, end-point devices warrant special consideration as part of the potential attack surface.

User Entity and Behaviour Analytics (UEBA) enabled end-point security solutions can help detect early signs of AI misuse and abuse by malicious actors. UEBA is known for its capability to detect suspicious activity by using an observed baseline of behaviour, rather than a set of predefined patterns or rules.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Vulnerability management

AI systems can be vulnerable at many levels, like the infrastructure running the AI, the components used to build the AI or the coded logic of the AI itself. These vulnerabilities can pose significant risks to the security, privacy and integrity of the AI systems, and you need to address them through appropriate measures.

Ensure to:

- Regularly apply software updates and patching to keep all software and firmware components of the AI infrastructure up to date.
- Conduct frequent assessments of AI infrastructure components, including hardware, software and data, to identify and remediate vulnerabilities in a timely manner.
- Conduct periodic penetration tests on the AI solutions and functionality.

Cybersecurity strategies to mitigate Artificial Intelligence (AI) risks

Security awareness

To improve resilience against threats and safeguard sensitive data, you need to foster a culture of security awareness. As with the advent of any new technology, you must ensure that all users understand the appropriate uses and the risks posed by AI technologies, and that security training materials are kept up to date with the rapidly evolving threat landscape.

Finnet
Building a Better Tomorrow, Today

Discuss areas you could apply the use of Artificial Intelligence in your Pension Scheme.

Questions & Answers

Every complaint and inquiry is a unique opportunity to build trust, refine governance, and deliver on our promise.

Thank You

ADDRESS

5th Floor, Crescent Business Centre (CBC), Parklands.
P.O. Box 48179-00100, GPO Nairobi, Kenya

CALL US

+254 719 560656, +254 740 257777, +254 111052230

WEB & SOCIAL

www.finnettrust.com | Facebook/LinkedIn: Finnet Trust