Finnet

Building a Better Tomorrow, Today

TOPIC : STRATEGIC RISK AND TECHNOLOGY RISK

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

INTRODUCTION

- Many business decisions come with risks. In order to understand all possible risks and rewards, many organizations have some type of risk management infrastructure to help them understand all possible outcomes of their decisions.
- Strategic risks are one type of risk that can positively impact performance and operations if executed correctly. Learning about these types of risks can help you decide if the company you work for may take them or how they can manage them better.

What is Strategic Risk

- Strategy risks, or strategic risks, are events or decisions that can affect different areas of the business.
- These are often decisions that companies take that can be dangerous, but the potential outcome can outweigh the risk.
- For example, making a large investment or acquisition can have some financial risk but when executed properly, it can have significant benefits.

Types of Strategic Risk

- **Reputational:** Reputational risks are ones that can affect public perception or employee engagement with a company.
- For example, a company may work in an endangered forest, risking its reputation among environmentalists, to make additional money.

Types of Strategic Risk

- **Governance:** Governance risks can affect the control, planning, and processes of a company.
- This might mean eliminating all current processes and starting with new documentation.

Types of Strategic Risk

- **Financial:** Financial risks are related to generating revenue and managing costs.
- One strategic risk might include selling a large piece of the business to improve operational costs.

Types of Strategic Risk

- **Competitive:** Competitive risks are when a company makes decisions about its branding and marketing initiatives so it can stand out among its peers. This can include investing in a new social platform or an innovative product design.

Types of Strategic Risk

- **Operational:** Operational risks can affect efficiency and help a company reduce waste.
- For example, a company might invest in a new system to automate tasks.

Types of Strategic Risk

- **Economic risk**: Economic risk refers to potential fallouts from a change in the economic landscape or legal framework within which a business operates.
- For example, lower government barriers to entry may allow new entrants to flood into the market, or high inflation may lead to a change in consumer behavior.

Types of Strategic Risk

- **Regulatory risk**: Regulations are being changed and added to all the time in the business sector. This provides an inherent risk as any failure to comply with a change in regulation could disrupt day-to-day operations or require the implementation of expensive new technologies.

Finnet
Building a Better Tomorrow, Today

HOW TO MANAGE STRATEGY RISK

1. Understand Risk Types

- To better manage risks around strategy, it can help to identify the other types of risks. Some risks businesses face include:
  - **Preventable risks:** Preventable risks are often internal and involve things that a company can control. Preventative risks include process breakdowns, error rates, or faulty equipment that a company may be able to fix before experiencing further issues.
  - **External risks:** External risks are factors outside of a company's control that can affect a business's performance or operations. These can include market volatility or political changes.
- Different from strategic risks, these other types require monitoring of internal and external factors rather than strategic decision-making.

2. Identify Strategy Risks

- Identifying these types of risks can be different from identifying other types, as they can often be positive. Understanding the company's customers, markets, and competition along with its individual strategic goals can help you identify these risks.
- For example, if your company goal is to increase revenue by 20% over the next five years, you can identify several risks you might face. With strategy risks, you can identify which risks you might take to help reach that goal.
- Consider brainstorming several risks you might take and what the potential positive and negative outcomes could be.

3. Perform Risk Assessments

- Once you've identified the risks, you can assess the magnitude of each. You might determine what the expected outcome is for each along with what might be the least favorable outcome.
- You can also assess both the likelihood of any issues you might face against the impact they could have. This can help you decide which risks you might take.
- For example, a company might pursue an investment that has a low chance of failure and a high impact.
- Consider gathering input from all business stakeholders, from finance to operations, to perform this assessment.

4. Determine A Plan

- For each risk, you can then determine how you might handle them. There are several strategies for handling risks:
  - **Acceptance:** Risk acceptance means pursuing a certain risk. When choosing this plan, you might discover that the risk for defects or cost impact is low, while the reward may be high enough to outweigh the risk.
  - **Transference:** Risk transference means pursuing a risk but placing the risk on an external company or individual. You may plan for this with events such as acquisitions, where you share initial cost burdens with another company.
  - **Avoidance:** Risk avoidance means avoiding taking a risk. After carefully evaluating the risks and rewards for a decision, you may determine it's a better business decision to avoid taking the risk.
  - **Reduction:** Risk reduction means adjusting the plan to minimize possible risks. For example, you might hope to release a new product into the market but may limit some functions first to see how the product performs.
- Whichever plan you choose for each risk, using information from your risk assessment can help you. Consider comparing the risk levels and determining how you might handle each option.

5. Develop a Framework

- Once you decide whether to pursue or avoid a strategic risk, you can establish a framework to help manage it.
- This involves gathering all the information about each risk and how you hope to handle them, determining who makes final decisions, and deciding on any safeguards you may implement take to minimize any issues.
- As an example, if you decide to pursue an acceptance strategy for a strategic risk such as making an investment, you can determine the key decision-makers, implement policies to ensure a smooth transition, establish ways to monitor progress, and create metrics to measure success.
- This framework can help evaluate the changing risk levels for the various strategic decisions a company might make.

6. Determine Metrics

- Once you've created your risk management framework, you can develop several metrics to help you make decisions, track progress, and monitor changes. Two metrics you might capture include:
  - **Economic capital:** Economic capital means having enough money to cover any potential losses a strategic risk might cost. If a company has enough economic capital, they may pursue these risks as the business could survive even if they don't reach their goals.
  - **Risk-adjusted return on capital (RAROC):** RAROC is an estimate of adjusted return on investment that helps businesses adjust their financial projections based on how risky an investment may be. This helps place a numerical value on potential investments that can change over time.
  - **Key performance indicators (KPI):** Key performance indicators are measurements that help an organization track progress toward strategic goals. Any changes in KPIs can show an organization whether high-risk decisions are successful or if they need adjustments.
  - **Key risk indicators:** Key risk indicators help companies with more than just strategic risks. Key risk indicators help businesses track any changes with internal and external risks, too. These can include changes in capital, customer engagement, or increased costs that can show when risk might increase for a company.

7. Monitor Progress

- When managing risks, it's important to monitor their changes regularly as internal and external factors can change.
- For example, if you hope to release a new product into the market and invest money into marketing, this can be a risk.
- By managing it, you can understand when the most effective time might be to release the product, depending on market conditions and current business performance, to maximize revenue and minimize costs.
- Consider reporting throughout these stages and while monitoring risks to identify changes and trends.

Finnet
Building a Better Tomorrow, Today

DIGITAL RISK REVIEW

INTRODUCTION

- Pension funds are fundamentally exposed to risk because of their business processes.
- This unavoidable exposure – or “inherent risk" – applies to all funds regardless of size.
- Understanding the nuances of how your fund operates is crucial to recognizing the cyber risks related to your services offered.

INTRODUCTION

- For instance, financial transactions and the handling of personally identifiable information constitute significant aspects of many organizations, and both bring with them inherent risks.
- If we examine a pension fund for example that provides services to active contributors and retired individuals, a broad spectrum of risk is dispersed across the entity.

INTRODUCTION

- Pension funds are usually recommended or required to conduct an annual actuarial assessment.
- This exercise involves meticulous scrutiny of various components like contributions, membership composition, and investment returns to determine funding levels.
- As pension funds supply this information to the actuary, they also inherit the third-party risk based on the actuary's risk mitigation capabilities.

INTRODUCTION

- Similarly, pension funds that deal with investment managers are exposed to third-party cyber risk.
- If these investment managers lack strong cyber controls, assets could inadvertently end up in the hands of threat actors.
- Likewise, providing member self-services, such as allowing members and annuitants to access information electronically, apply for loans, or update beneficiaries, could also expose organizations to cyber threats.

What does cyber risk mean for pension schemes

- The Pensions Regulator defines cyber risk as the *'risk of loss disruption or damage to a scheme or its members associated with using information technology'*.
- This means not only the technology itself but also the people using it and the processes supporting it.
- It is clear therefore that pension schemes are expected to understand, assess and manage the level of risks to which they are exposed

Why are pension schemes, trustees and their suppliers attractive to potential cyber criminals

- Pension schemes, trustees and their suppliers are attractive targets to cyber criminals because:
  - Trustees control (usually indirectly) rich levels of personal data and will typically have a highly complex and multi layered set of processes to manage trustee assets in order to deliver scheme benefits to their ultimate end-users - the scheme members. This data can easily be monetized or weaponized against trustees or scheme members (through the threat of misuse).
  - Trustees are inherently reliant on a number of different service providers, including the administrators, asset managers, payroll providers etc. in order to fulfil their legal duties and ultimately, their obligations to members. This means trustees' defenses against cyber risk are only as strong as the weakest link in their supply chain

How do cyber criminals attack pension schemes, trustees and their suppliers and what is the impact

- In the pension scheme context, a cyber incident will typically (but by no means only) involve:
  - Hackers gaining access to computer systems (usually a scheme administrator or other supplier) and exfiltrating data.
  - Introduction of 'ransomware' - encryption of systems via malware, which can only be unlocked upon payment of ransom.
  - Phishing attacks (usually in response to phishing) where data processors may be tricked into releasing data.

How do cyber criminals attack pension schemes, trustees and their suppliers and what is the impact

- Consequences of a cyber attack can range from direct theft of pension scheme assets, the threat of theft (of data or assets) or disruption in payment of benefits (and members suffering exposure to risks of identity theft).
- Cyber incidents can therefore have devastating consequences not only for scheme members but also for trustees and their suppliers from a financial, legal and reputational perspective

Regulatory Priorities: ITA & RBA

- Trustees may want to keep this front of mind when dealing with either regulator in the context of a cyber incident.
- **ITA**
  - The ITA's primary focus is to ensure the rights and freedoms of individuals are protected – this is their 'north star' and guides their enforcement approach.
  - Following a notification, or awareness of an incident – the ITA will consider whether to launch an investigation. The focus will be on whether the entity in question had, 'appropriate' technical and organizational measures in place, to protect personal data. These measures need to be commensurate to the risks posed. This is called the 'security principle' and applies to both data controllers as well as data processors.
  - Given the increase in cyber incidents the ITA has moved towards closing their files for 'smaller breaches' relatively quickly – sometimes within a matter of days. However, some organizations undergo years of regulatory investigations, occasionally resulting in large fines.

Regulatory Priorities: ITA & RBA

- **RBA**
  - RBA is focused on ensuring employers, trustees, pensions specialists and business advisers can fulfil their duties to scheme members.
  - In a cyber incident context – key focuses include ensuring pensions and other beneficiaries are paid on time.
  - RBA is also focused on ensuring the administrative services experiencing disruption are returned to normal – as soon as possible. It is important that business continuity planning and disaster recovery processes are well rehearsed to mitigate the risk here. This is something RBA is focusing on more and more.

The Landscape of Digital Risk

- A key part of this operational resilience is the ability to manage risks associated with an increasing reliance on digital business practices.

The Landscape of Digital Risk

- Digital risks include those related to software and hardware, such as service outages or unauthorized access.
- But they also include risks related to the application of digital technology.
- Consider the following examples:
  - **Retail lending:** An artificial intelligence (AI) system processes a high volume of inputs through hundreds of steps to arrive at a lending decision. But it isn't clear that the decision is fair—and between the system's complexity and its ability to learn on its own, it can be extremely difficult to understand why the system behaves as it does.

The Landscape of Digital Risk

- **Derivative trading:** Two parties agree to a simple interest rate swap through a blockchain.
- They set up a smart contract that transfers value at the end of each settlement period based on market data from a central authority.
- However, the blockchain authenticating the trade potentially exposes the details of the trade to competitors.

The Landscape of Digital Risk

- **Underwriting:** Facing declining margins, a life insurance company turns to emerging markets where the potential for growth is significant.
- However, these locations have no agent networks, making mobile technology the practical way to reach customers.
- The insurer partners with a fintech firm to develop an app, only to find itself disintermediated as the partner gains control of the customer relationship

The Landscape of Digital Risk

- As these examples indicate, digital risk can be strategic, financial, operational, regulatory, or reputational in nature.
- Digital risk is also highly nuanced and subject to ongoing change as digital ecosystems, business, and service models evolve.

The Landscape of Digital Risk

- The examples also reveal a tension at the heart of operational resilience.
- On the one hand, it demands that firms mitigate the new digital risks they're exposed to.
- On the other hand, operational resiliency more broadly reflects the firm's ability to respond to fast-changing business conditions.

The Landscape of Digital Risk

- The implications include:
  - New culture and skills for informed risk taking and experimentation
  - New frontiers of engaging in a vast and complex global ecosystem
  - New speed of execution when near continuous change is the norm
  - New accountabilities for operating in the physical and digital domains
  - New ethics in the wake of opportunities and challenges that didn't exist before.

Finnet
Building a Better Tomorrow, Today

TYPES OF DIGITAL RISK

Cybersecurity Risk

- As processes and data become more digitized and networked, cybersecurity risk goes up.
- Firms may exacerbate the risk by trying to protect all digital assets equally rather than shifting more protection to the "crown jewels."
- They may also focus on avoidance of cybersecurity incidents at the expense of mitigation strategies, and vigilance at the expense of ease of doing business.

Ecosystem Risk

- Business ecosystems creates more opportunities for cyber-intrusion and systemic risks.
- For instance, partnerships and outsourced services can boost organizational exposure to bad actors, contagion, and errors from model miscalibration.
- Meanwhile, systemically important technology and data providers can introduce single points of failure.

Emerging Technology Risk

- The greatest digital risks may be from technologies that don't exist yet.
- Think financial exclusion as technology systems invent their own logic, unintentional collusion as institutions interact through high-speed networks, and breach of fiduciary duty as digital systems take on broader sets of customer-facing responsibilities.

Execution Risk

- To be successful, digital projects require fundamental, top-down shifts in how organizations execute.
- Without those shifts, firms may run into challenges with user adoption, institutional buy-in, and integration with legacy systems.
- In addition, organizational structures may hamper rather than support agile execution.

Fraud Risk

- Amid increasing volumes of digital transactions—especially cross-border ones—strong know your customer (KYC) and anti-money laundering (AML) processes become more important than ever.
- They help fight fraud associated with open banking, money transfers, new account activation, and more in an environment where it can be unclear who owns the liability of fraud.

Privacy Risk

- Data is proliferating—and so are laws around data privacy and transparency.
- Between them, these two trends raise the stakes of a data breach involving personally identifiable information. Retention of unnecessary data can add to the risk.
- So can a lack of clarity on data ownership, uses, and alteration.

Legal and Regulatory Risk

- Around the world, regulators are issuing new rules addressing the increasing digitization of financial services.
- These regulatory regimes are in various stages of maturity and may contradict existing business practices.
- A rush to comply can add to the risk by creating complex, overlapping layers of compliance requirements and systems.

Brand and Reputational Risk

- Data loss, outages, and misuse can significantly impair a financial institution's reputation.
- Beyond that, digital tools may introduce ethical pitfalls and biases that can reflect negatively on financial services.
- Examples include incomplete or unrepresentative data sets, bias in input data, and subconscious developer bias that influences the internal logic of a digital application.

Strategic Risk

- Strategic choices can intensify digital risk.
- For instance, firms may opt not to integrate their IT and business strategies.
- They also may opt to digitize existing processes without improving them or emphasize short-term cost savings over an upgrade of the full digital environment.
- Another choice might be to ignore new partners and technologies rather than embrace them.

People and Culture Risk

- Talent to support digital transformation— examples include data scientists and developers—can be in short supply.
- At the same time, opportunities to upskill or cross-train staff may be limited.
- Some employees may resist digital transformation for fear of losing their jobs, while long-term trends may prompt financial institutions to accommodate more flexible ways of working.

Turn Digital Risk into Digital Advantage

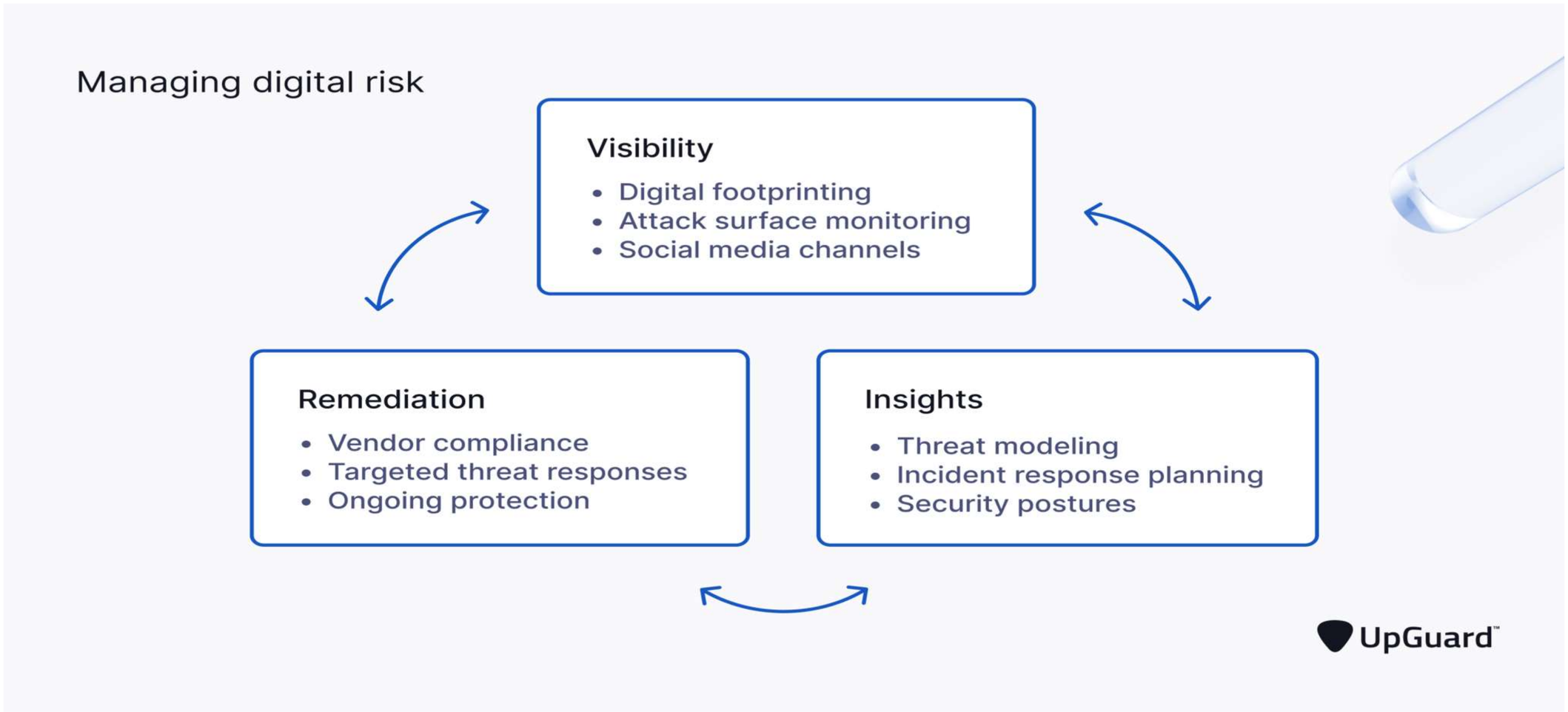
- So where can boards take it from here? Consider any of the following actions as a starting point:
  - Form a board-level committee to promote understanding of digital risk
  - Add a board director with strong digital management skills and leadership experience
  - Call for internal audit to report on digital risk via the audit committee
  - Encourage management to enhance the quality of reporting on digital transformation
  - Define thresholds for digital risk situations that merit board-level attention
  - Make room on the board meeting agenda for a discussion around digital risk
  - Require management to give a plain English update of digital risks, programs, and issues
  - Bring in guest speakers to provide independent views of the digital risk landscape
  - Stress-test the organization's capabilities to respond to a major event

Managing Digital Risks

- Effective digital risk management is a cyclical effort between visibility, insights, and remediation, where each quadrant is powered by the data obtained from the preceding quadrant.
- Visibility is achieved through digital foot printing to monitor exposed assets. Visibility data is fed through threat intelligence solutions to power insights into the best remediation responses.
- Digital landscape insights empower the design and deployment of highly-effective remediation responses.

Finnet
Building a Better Tomorrow, Today

Managing Digital Risks



Step 1. Identify All Exposed Assets

- Identify all assets exposed to potential unauthorized access.
- This should include all social media channels and resources housing sensitive data.
- A digital footprint can be mapped with the assistance of an attack surface monitoring solution.
- Critical assets at risk of exposure can include:
  - Social media channels
  - Critical data (customer data, employee data, health information, financial information, etc.)
  - Shadow IT
  - Cloud platforms

Finnet
Building a Better Tomorrow, Today

Step 2. Monitor for Data Leaks

- A data leak detection solution can discover any data leaks linked to your organization to provide both visibility and vulnerability insights into this commonly overlooked attack vector
- Cybercriminals are always searching for data leaks to arm their data breach campaigns.
- By remediating data leaks before cybercriminals discover them, cybersecurity, and therefore all other categories of digital risk, will be protected.

Step 3. Keep Risk and Threat Models Updated

- With a digital footprint established, all threat intelligence data can be collected to create a model of your threat landscape.
- In addition, to improve cyber resiliency, organizations should also consider reviewing their incident response, business continuity, and disaster recovery plan to ensure all security teams can respond to all potential cyber risk factors.
- Businesses should also update these cyber resiliency plans every time their threat model is refreshed.
- Best practices suggest that these security policies are reviewed consistently, on at least an annual basis.

Step 4. Secure Access to All Exposed Resources

- To protect against reputational damage, privileged accounts and digital assets should be protected from compromise.
- Rather than only focusing on established cyber defenses around sensitive resources, detection parameters should be broadened to detect and block all unauthorized network access.
- This also involves access control for internal usage as well. Controlled privileges allow organizations to prevent unauthorized employees from accessing critical data beyond their job roles, reducing the risk of insider threats as well.
- Strategically placed honey tokens will alert organizations to any unauthorized access attempt. Further access to resources can be mitigated with a Zero Trust Architecture (ZTA), an assume breach mentality and enhanced Privileged Access Management (PAM) security.

Step 5. Keep Vendors Compliant

- The risk of non-compliance has both a financial and cybersecurity impact. Non-compliance is linked to poor security efforts.
- To mitigate the risk of non-compliance, it's not enough to only monitor the internal ecosystems, the entire vendor network needs to be purged of security vulnerabilities.
- Organizations need to perform their vendor due diligence to ensure that all new and existing third parties in the supply chain are properly evaluated and assessed.
- Cybercriminals could breach your organization through vendors with poor security postures.
- A third-party risk management solution will ensure all vendors remain compliant through regulatory-specific risk assessments.

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