THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

Internal Audit Beyond Compliance:

Safeguarding Tanzania's Digital Economy

Beyond compliance: How internal audit can tackle cybersecurity and digital risks in Tanzania's growing economy

Tanzania's economy is changing fast. Mobile money has reshaped how people pay and save. Fintechs are widening access to financial services. E-government platforms are changing how citizens and middle-market organisations interact with public institutions. Small and medium-sized middle-market organisations are moving sales, records, and customer engagement online. This digital progress is creating real opportunity, but it is also creating a new risk landscape.

Cybersecurity incidents, digital fraud, weak data controls, and poor technology governance no longer sit at the edge of business risk. For boards, chief executives, chief financial officers, and audit committees, this changes what they must ask of internal audit. A compliance checklist is no longer enough. Internal audit must move beyond backward-looking assurance and become a forward-focused function that helps organisations manage digital risk with clarity and confidence.

Tanzania's digital risk landscape is growing in complexity

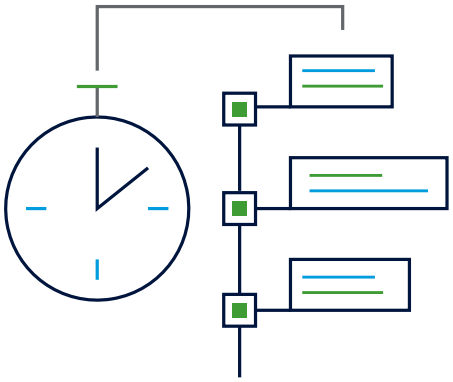
Digital adoption in Tanzania brings scale, speed, and access. It also brings exposure and the pace is accelerating.

Cyber threats are rising with digital usage

As more transactions move online, cyber criminals gain more entry points. Phishing attacks, social engineering, payment fraud, account takeover, and insider-enabled fraud are increasingly relevant in Tanzania's market. Mobile money platforms, digital wallets, and online banking channels are especially attractive targets because they combine high transaction volumes with time-sensitive customer behaviour.

For many organisations, the risk is not a sophisticated external attacker. It is a weak password, poor user access control, a staff member who clicks a malicious link, or a process gap between operations and information technology teams.

A growing retailer that accepts digital payments, for example, may invest in customer-facing technology but fail to review who can access its payment systems, how exceptions are monitored, or how incidents are escalated. That gap can lead to financial loss, customer distrust, and regulatory scrutiny.



Artificial intelligence and automation create new risks

AI enabled tools are entering Tanzanian organisations through two channels: direct adoption by management and embedded features through third party softwares. Artificial intelligence is influencing decision-making, customer service, fraud detection, reporting, and back-office processes.

The opportunity is clear, but so is the risk. If management does not understand how tools make decisions, where data comes from, or how outputs are reviewed, the organisation may create new errors at speed. Bias, poor data quality, weak oversight, and unclear accountability can quickly become governance problems, not just technology problems.

Data privacy expectations are increasing

Data protection is becoming more important across industries. Tanzania's Data Protection Act and other regulators has raised the standard of how personal data must be collected, stored, processes and protected. . Yet many organisations building practical compliance capabilities have not kept pace with their legal obligations

That creates a common gap. Policies may exist, but data mapping is incomplete. Consent processes may be unclear. Sensitive data may sit in spreadsheets, shared folders, personal devices, or third-party systems without adequate control.

For public institutions, banks, telecom operators, healthcare providers, and digital middle-market organisations, this is a material risk. For small and mid-sized middle-market organisations, it is often an overlooked one.

Governance weaknesses can amplify digital risk

In many emerging market environments, digital risk grows faster than governance maturity. Technology moves quickly, while board oversight, risk reporting, internal controls, and staff capability move more slowly.

This affects all types of organisations:

- Small and medium-sized middle-market organisations often digitise before they formalise controls.
- Larger corporates face complexity from scale, third parties, and legacy systems integration.
- Public institutions carry high levels of sensitive data and public trust obligations.

In many emerging market environments, digital risk grows faster than governance maturity. Technology moves quickly, while board oversight, risk reporting, internal controls, and staff capability move more slowly.

The lesson is simple: digital risk is no longer only an information technology issue. It is an enterprise risk.

Why traditional internal audit is no longer enough

Many internal audit functions still approach digital risk through a narrow lens. They review policy compliance, test selected controls, and report after the fact. That work still remains necessary but is not sufficient on its own.

Annual audit cycles can't keep pace

Cyber and digital risks change quickly. A risk assessment carried out once a year may already be out of date a few months later. New applications, vendors, interfaces, and fraud patterns can emerge much faster than traditional audit plans can respond.

Without more dynamic monitoring, internal audit risks reporting on yesterday's weaknesses while management faces today's threats.

Skills gaps remain a real challenge

Many internal audit teams are strong in finance, process, and compliance, but less confident in cybersecurity, technology risk, data governance, or artificial intelligence oversight. That creates blind spots.

The issue is not that every internal auditor must become a cyber specialist. The issue is that every internal audit function now needs enough digital fluency to ask the right questions, interpret the right evidence, and know when to bring in deeper expertise.

Information technology audits often sit apart from business audits

One of the most common weaknesses is separation. Information technology audits happen in one lane. Operational or financial audits happen in another. But digital risk doesn't work that way.

A procurement audit, for example, should consider vendor system access, data sharing, and system workflow overrides. A payroll audit should consider privileged access, change management, and cyber fraud scenarios. A revenue audit should consider digital payment integrity and customer data protection.

When audit work stays fragmented, risk stays hidden. And in a digital environment, hidden risk tend to crystallise quickly.

The shift: internal audit as a strategic partner

Internal audit now has an opportunity to create stronger value. That starts with a broader mandate and a clearer point of view.

Move from assurance alone to assurance and foresight

Internal audit must still provide independent assurance. But leading functions also help management and boards see what is changing, where control frameworks are falling behind, and what action matters most.

That means bringing insight, not only findings. It means highlighting emerging risks, not only historic gaps.

Embed cyber and digital risk into all audits

Cybersecurity should not sit only in a stand-alone cyber review. It should be embedded across the audit universe wherever digital dependency exists, which is now almost everywhere.
Internal audit should ask:

- What systems support this process?
- Who has access?
- What data is involved?
- Where could fraud occur?
- How would management know if something went wrong?
- Are third parties introducing hidden exposure?

This approach gives boards a more realistic view of risk.

Support better decision-making at board and management level

Boards don't need technical detail for its own sake. They need clear insight into business impact, risk exposure, control effectiveness, and response readiness. Internal audit is well placed to translate digital risk into language decision-makers can act on.

This is where internal audit creates value. It helps leaders balance growth, resilience, and trust.

Practical actions for Tanzanian organisations

Organisations that want to strengthen their resilience should focus on the following priorities:

Strengthen cybersecurity governance

Set clear accountability for cyber and digital risk. Management should define ownership, escalation routes, incident response roles, and reporting expectations. Boards and audit committees should receive clear, regular updates on the risks that matter most.

Build digital risk into audit planning

Audit plans should reflect the organisation's digital footprint, not just its traditional control cycle. Internal audit should give more attention to high-risk systems, payment processes, third-party platforms, data flows, and change programmes.

Improve staff awareness and cyber culture

Many incidents begin with human behaviour. Staff need regular, practical guidance on phishing, fraud red flags, password discipline, remote working controls, and incident reporting. Culture matters as much as technology.

Use data analytics in audit work

Internal audit should make greater use of data analysis to identify unusual transactions, control exceptions, access anomalies, and patterns that may point to fraud or weak oversight. This helps audit move closer to real-time assurance.

Use artificial intelligence carefully and with control

Where audit teams use artificial intelligence or automation, they should do so with discipline. Tools can improve coverage and efficiency, but they still need human review, data quality checks, and clear governance.

Improve reporting to boards and audit committees

Board reporting should be concise, relevant, and risk-based. Focus on exposure, impact, trends, response readiness, and management action. Leaders need clarity, not technical overload.

A practical perspective from RSM Tanzania

Across the market, we see a clear pattern. Organisations often know digital risk is rising, but they are less certain how to reshape internal audit in response. This is where external perspective can help. At RSM Tanzania, we support organisations through internal audit transformation, cybersecurity assessments, technology risk reviews, and broader risk advisory.

Our approach is collaborative and practical. Wedo not replace internal audit function, but we strengthen it with the methods, tools, and specialist insight needed for a more digital environment.

That support is especially valuable where organisations are growing quickly, adopting new systems, facing regulatory change, or trying to modernise audits without losing independence and rigour.

Conclusion

Tanzania's digital economy is full of promise. It is expanding access, improving efficiency, and opening new paths to growth. But digital progress also raises the stakes for risk management, governance, and assurance.

Digital risk is business risk. It affects revenue, clients, reputation, compliance, strategy, and trust. That is why internal audit must move beyond compliance and take a broader, more strategic role. When internal audit combines independence with insight, and assurance with foresight, it helps organisations respond to risk with confidence and move forward with greater resilience.

Tanzania's digital future will reward organisations that grow securely, govern technology well, and act early. Internal audit has a real opportunity to lead that shift.

Disclaimer:

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

DAR ES SALAAM

1st Floor, Plot No. 1040,
Haile Selassie Road, Masaki
P.O. Box 79586,
Dar es Salaam, Tanzania
Tel: +255 22 2602714 / 2602774
Email: info@rsmtz.co.tz
Website: www.rsm.global/tanzania
Contact: Lina Ratansi (Managing Partner)

ARUSHA

2nd Floor, West Wing
Goliondoi Road, Ngorongoro Tourism Centre
P.O. Box 14512,
Arusha, Tanzania
Tel: +255 22 2602714 / 2602774
Email: info@rsmtz.co.tz
Website: www.rsm.global/tanzania
Contact: Lina Ratansi (Managing Partner)

Follow us for news and more updates on:

RSM Tanzania @rsmtanzania RSM Tanzania