CIGFARO Mpumalanga

Pre-Audit & Performance Webinar 2026

Leading sustainable improvement through internal controls

Presented by:
Thina Naki,
mSCOA Technical Advisor

Institution:
National Treasury

Date:
23 July 2026

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

*m*SCOA Regulation 2014

- As mandated by National Treasury, *m*SCOA structures municipal financial data within a multi-dimensional classification framework.
- It facilitates the integration of budgeting, transacting, and reporting processes.
- It enhances oversight, accountability, and consistency in municipal recording and reporting.
- It establishes a standardised framework for budgeting, recording, and reporting across municipal systems.
- It supports informed decision-making, benchmarking, and compliance with MFMA requirements.
- It enables municipalities to make accurate, evidence-based decisions that respond to community needs.

Next phase in *m*SCOA Reform Agenda (1)

- *m*SCOA Regulations states that Minister of Finance may, by notice in the Gazette, determine the minimum business process and system requirements for LG to enable implementation of the regulations
- National Treasury has embarked on a project in Jan 2024 to:
  - Review and update the minimum business processes and technical system specifications in MFMA Circular No. 80 (2016); and
  - Develop standard operating procedures (SOPs) for *m*SCOA;
  - Develop the following position papers to address common challenges, reducing ambiguity, and promoting consistent interpretation:
    - Municipal System Integration
    - Use of Core Solution Chart of Accounts as a Base for Source System Integration
    - Data Migration, Conversion and Management
    - Defining Upgrade versus New System Implementation

Next phase in *m*SCOA Reform Agenda (2)

- To date, the following consultation has taken place with various stakeholders, including municipalities, various NT units, PTs, system vendors, AGSA, SARS, STATSSA, DCoG, DWS, etc.:
  - Technical working groups (88 engagements)
  - Integrated Consultative Forums (14 engagements)
  - Stakeholders Engagements (18 engagements)
  - Special Task Team meetings (10 engagements)
  - Training sessions (7 sessions)
- Link to consultation documents: G1_Draft Regulations - Training

Timelines for issuing of the minimum business process and technical system requirements for *m*SCOA

2024 – 2026

Commence and conclude work to:

- Review/determine minimum business processes and system requirements for *m*SCOA
- SOPs
- Position Papers
- ICT Due Diligence Assessment

2026 – 2027

- Provincial training on minimum requirements
- Issue position papers as MFMA circulars
- Issue updated ICT Due Diligence Assessment

2027 – 2030

- Issue minimum requirements for implementation
- Readiness Workshops
- Readiness assessments (by municipalities and vendors)
- Monitoring of progress against *m*SCOA Road Maps
- Handholding
- Issue transversal tender

2030 - 2035

- Phased implementation: 3 - 7 years
- Handholding
- Training
- Compliance Assessments

Minimum business processes and system requirements for *m*SCOA - Governance

To improve the quality of audit and reporting information

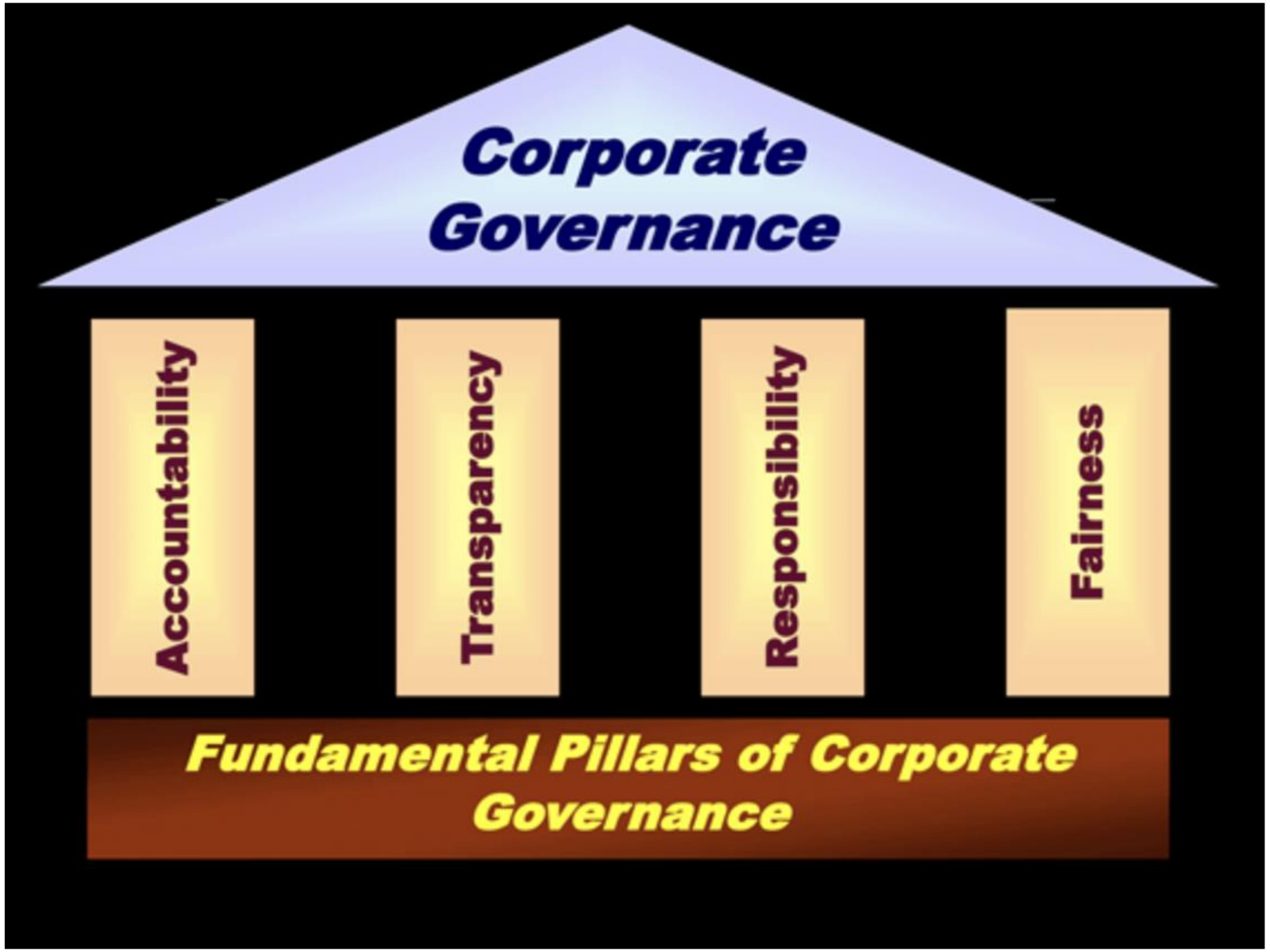
Accessibility to electronic documentation (purchase orders, requisitions, approved payment vouchers, supplier invoices, SLAs etc)

Reduction in direct journals on GL – all transactions and corrections to happen in submodule and direct alignment to GL

Automation of registers and reconciliations (Loans register, creditors recon, creditors listing, investment register, grant register, among others)

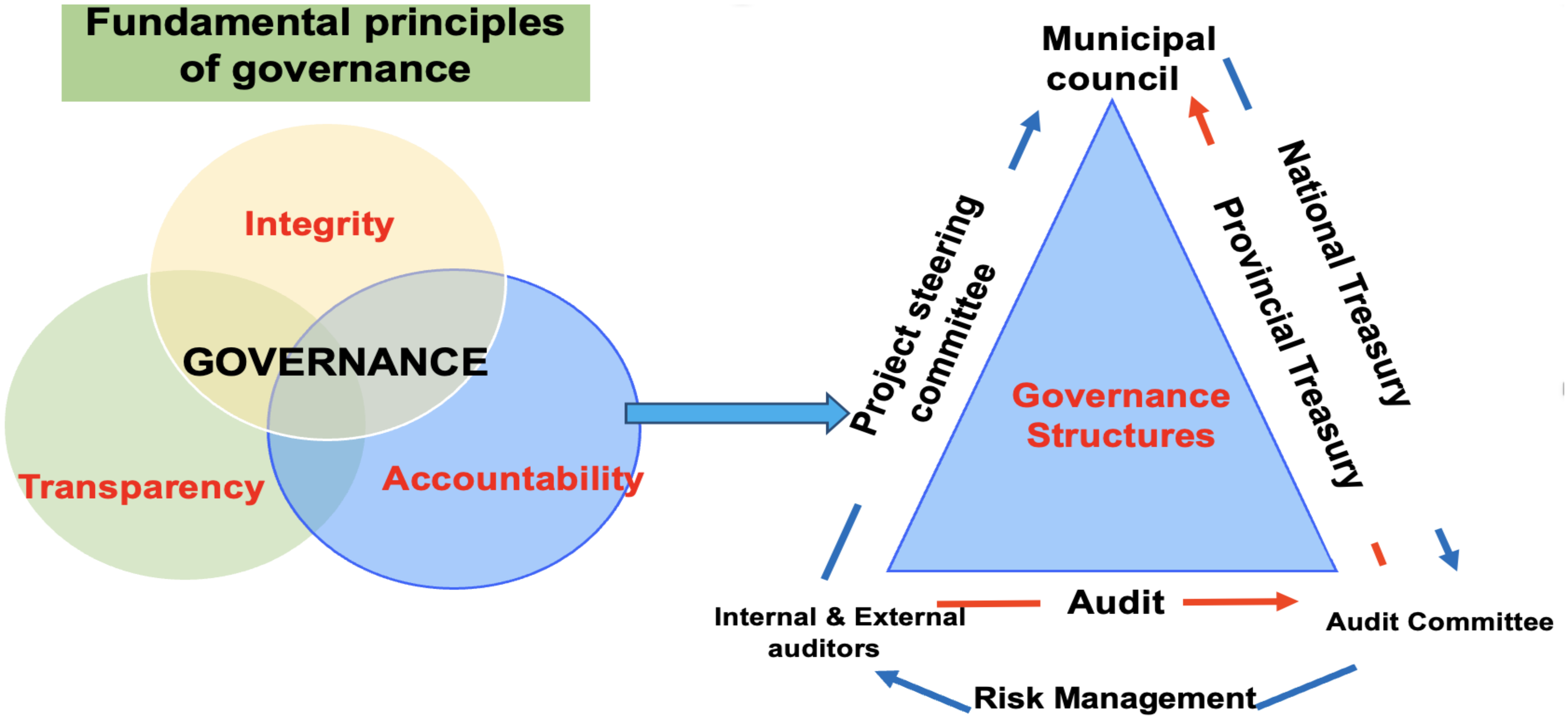
Reduce audit queries – standardised systems in terms of reporting and functionality – processes embedded in systems

Corporate Governance



Governance structures

In a *m*SCOA environment, good governance is strengthened through collaboration of the governance structures:



System requirement groups for Corporate Governance Management and Reporting

Purpose of system requirements & functionalities for *m*SCOA

- Enhance audit efficiency, improve the quality of audit evidence, and support risk-based sampling in line with applicable standards, while preserving the integrated municipal system solution security
- Secure, read-only access or controlled data replication mechanisms (such as secure views, reporting layers, or approved data integration services) that prevent any ability to alter transactional data. *Appropriate safeguards, including segregation of duties, access controls, system authentication, and audit logging, must be embedded to mitigate risk*
- Requirements are aligned to the Global Internal Audit Standards (GIAS) as well as the topical requirements and are part of the business processes/system functionalities/ activities. *The GIAS focuses on fundamentals, which also prioritise engagement findings based on significance and the use of ratings*
- Reduce the effort of manually populating various reports with the same information and should ideally automate the details from the system. The reporting format for the various commitees, management and MPAC maybe customised or embedded by the municipality/municipal entity based on requirements

Integration between the municipal system solution and third-party service providers

- Integration means the electronic linkage of data, processes, and functionalities within a municipal system solution, or between the municipal system solution and external platforms, to enable the secure, accurate, and real-time or scheduled transfer of information
- Sensitive data, including data relating to personal data, must be treated with the appropriate level of security, in line with legislation such as the POPIA Act
- Where municipalities engage third-party service providers, integration must ensure that data originating from these providers is transferred seamlessly into the municipal system environment without compromising the principle of One Source of the Truth

Internal Audit function

Internal audit management is a key governance process that strengthens internal controls, enhances financial integrity and supports the prevention and detection of irregularities within municipalities and municipal entities.

Internal Audit Role

Must review the implementation of *mSCOA* Business processes and system requirements to ensure that:

- The process of incorporating controls within integrated systems is done.
- Ensure that proper classification and approval workflows are being followed.
- Role-based access is implemented as an effective measure to limit unauthorised transactions.

These controls are designed to reduce the risk of fraud, errors and non-compliance.

Role of Internal Audit in preparation for the minimum *mSCOA* requirements

- As part of assurance provisions, internal audit must review the municipal *m*SCOA roadmap to ensure alignment to the minimum requirements for *m*SCOA
  - I.t.o. the *m*SCOA Regulations (2014) and MFMA and *m*SCOA circulars
  - The proposed minimum requirements that will be issued shortly (as per consultation documents G1_Draft Regulations - Training
- Verify that the roadmap is aligned to MFMA Circular No. 80
- The roadmap is aligned to MFMA Circular No.126 and addresses the following aspects:
  - ICT architecture requirements
  - Governance and Institutional Requirements
  - System Functionality requirements
  - User Proficiency and Training
  - Change management

Audit committee

The audit committee plays a pivotal role in corporate governance, offering independent oversight of key areas such as financial reporting, internal controls, risk management and compliance.

Audit committee

The Audit committee fulfils its role through:

- Compliance oversight: Monitor *mSCOA* Steering and ICT committee and to ensure that system-compliance audit queries are addressed.
- Risk management: Verify technology risks ensuring that risk management process has been adequately done.
- Control assurance: Reviewing controls over automated data transfers to ensure information is secure, accurate, and aligned with National Treasury requirements

External Audit

- **Encourage Coordination Across Assurance Providers:** external audit, risk management, and compliance functions
- The coordination will strengthen governance, internal control, audit readiness, and risk oversight across municipalities and municipal entities

External Audit

External audit management and reporting help municipalities maintain transparency, accountability, and compliance with public sector requirements by:

- Independently verifying compliance with NT regulations by verifying:
  - System Integration (that no manual uploading is allowed).
  - Data Integrity (Correct segment combination)
  - Audit trails (system securely logs who changes data, what they change, and when.
  - Compliance with *mSCOA* Regulations
- That there are role-based access configuration, allowing system administrators to assign specific permissions such as edit, view-only, or notification access, based on the user’s job function and approved delegation of authority.

Risk Management

Implementation of *mSCOA* business processes and system requirements enables better identification and monitoring of financial and operational risks through:

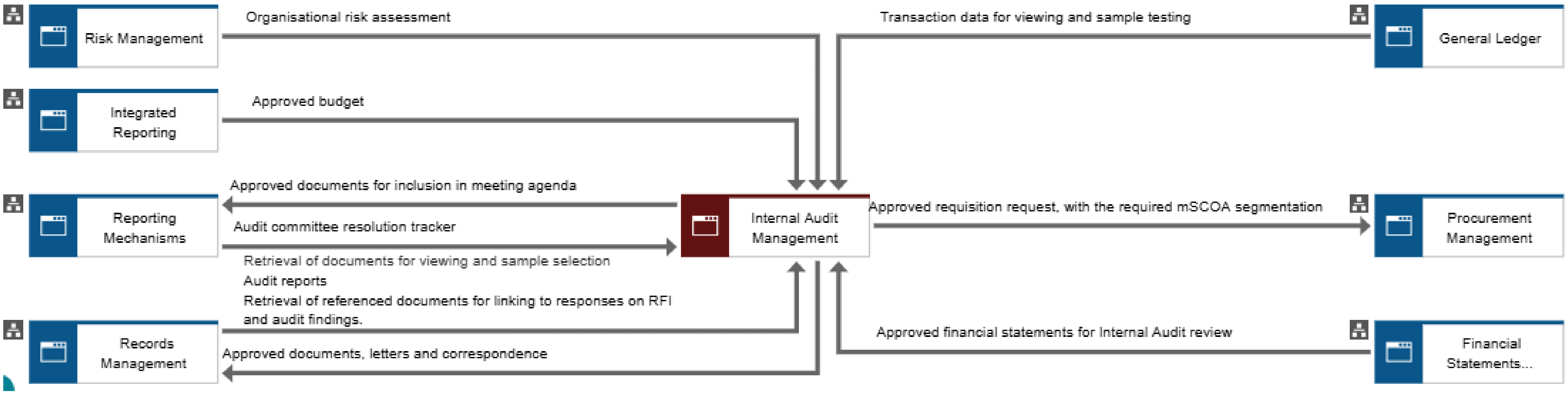
- Detailed transaction-level data
- Improved reporting capabilities
- Alignment between budgets, expenditures, and projects

This allows risk management and internal audit functions to focus on high-risk areas and provide targeted assurance.

Benefits of compliance with *mSCOA* business processes and system requirements

- Reduced manual errors and data manipulation
- Enables accurate and complete financial records
- Strengthens audit trails
- Reduces the duplication of audit and review efforts
- Superior risk coverage and reduces blind spots
- Improved quality and reliability of information
- Achieving cost efficiency in assurance activities
- Enhanced governance and decision-making processes

Key Integration Requirements



Future considerations

The responsibilities of Internal Audit taking into consideration *m*SCOA

- It is important to emphasise that *m*SCOA is not limited to a finance reform initiative, but constitutes an organisational reform aimed at ensuring a single version of the truth is maintained and reported on, both internally and externally.
- Internal audit plays a critical, independent assurance role in a Municipal Standard Chart of Accounts (*m*SCOA) environment by validating system compliance, data integrity, and operational efficiency.
- Internal audit provides independent assurance on the effectiveness of these controls and supports detection through audits and data analytics.

Conclusion

Through strengthening and maintaining good governance and accountability and ensuring that all the governance structures work together cohesively through fulfilling their mandate of providing oversight to the municipalities, *mSCOA* compliance can be achieved

THANK YOU

For additional information on municipal matters, visit the MFMA Webpage at http://mfma.gov.za or

https://lg.treasury.gov.za/ibi_apps/welcome

https://municipalmoney.gov.za

For additional information on national and provincial budgets, visit: https://vulekamali.gov.za

ANNEXURES

Key Principles in System Requirements (1)

Review the Internal Audit Function

- Enable electronic planning, scheduling and management of internal audit reviews, including approval workflows, scope definition, risk-based planning and assignment of audit resources.
- Provide functionality to capture, document and assess internal audit methodologies, independence, staffing capacity, quality assurance processes and compliance with legislative and professional standards. Support electronic working papers, evidence management and linkage of internal audit findings to risk registers, audit action plans and governance oversight structures.
- Enable structured tracking of internal audit findings, recommendations and management responses, including progress monitoring, milestone tracking, escalation and full audit-trail logging. Provide dashboards and reporting to evaluate internal audit performance, implementation of recommendations, quality review outcomes and alignment with the annual internal audit plan. Implement role-based access control, segregation of duties, document version control, secure storage and long-term archiving aligned with MFMA, governance and oversight requirements. Enable integration with external audit management, audit action plan systems and records management platforms to ensure coordinated assurance reporting.

Key Principles in System Requirements (2)

Conduct Internal Audit Planning

- Enable development and approval of a risk-based Internal Audit Plan aligned to the organisational risk register, strategic objectives, legislative requirements and prior audit outcomes. Provide functionality to capture, prioritise and schedule planned internal audit engagements, including scope definition, resource allocation, timelines and approval workflows.
- Support integration with the enterprise risk management system to identify high-risk areas, emerging risks and recurring findings for inclusion in the audit plan. Enable collaboration and consultation workflows with management, audit committees and oversight structures during the planning process, including version control and approval tracking.
- Provide dashboards and reporting to monitor implementation of the approved Internal Audit Plan, resource utilisation, plan amendments and alignment with governance requirements. Ensure secure document management, audit-trail tracking, role-based access control and long-term archiving of internal audit planning documentation.

Key Principles in System Requirements (3)

Execute internal audit assignments

- Enable structured execution of internal audit assignments, including task allocation, time tracking, progress monitoring and supervision of audit team activities. Provide electronic working paper functionality to perform audit testing, capture procedures performed, record results and upload supporting audit evidence with full version control and audit-trail tracking.
- Support documentation and evaluation of internal controls, risks and compliance with legislation, policies and procedures during audit execution. Enable structured capture, review and approval of audit findings, root-cause analysis and recommendations prior to reporting.
- Provide workflow functionality for quality review, supervisory review and sign-off of completed audit work and working papers. Ensure secure storage, role-based access control, segregation of duties and long-term archiving of internal audit execution documentation aligned with governance requirements.

Key Principles in System Requirements (4)

Review structure of internal audit report

- Enable automated compilation of internal audit reports using standardised templates, including audit scope, methodology, findings, recommendations and management responses
- Provide workflow functionality for review, quality assurance and approval of internal audit reports, including version control, electronic sign-off and full audit-trail tracking. Support secure distribution of approved internal audit reports to management, audit committees and oversight structures with controlled access and confirmation tracking
- Enable linkage of reported findings to risk registers, audit action plans and follow-up monitoring processes to ensure implementation tracking and accountability
- Provide dashboards and reporting to monitor status of issued reports, implementation of recommendations and overall assurance outcomes. Ensure secure storage, records management integration, role-based access control and long-term archiving of internal audit reporting documentation

Key Principles in System Requirements (5)

Report to Audit Committee and stakeholders

- Enable automated compilation of audit committee and stakeholder reports using standardised templates, incorporating internal audit results, audit findings, risk information and implementation status of action plans.
- Provide workflow functionality for review, approval and electronic sign-off of reports prior to submission to the Audit Committee and relevant oversight structures. Support secure electronic distribution of approved reports, meeting packs and supporting documentation with controlled access and confirmation tracking.
- Provide dashboards and analytics to monitor implementation of audit committee resolutions, status of audit findings and progress against governance and assurance plans. Ensure secure storage, role-based access control, records management integration and long-term archiving of audit committee and stakeholder reporting documentation aligned with legislative and governance requirements.

Key Principles in System Requirements (6)

Undertake follow-up audit reviews

- Enable scheduling, planning and management of follow-up audit reviews linked to prior audit findings, recommendations and approved action plans, including automated reminders and escalation of overdue items. Provide functionality to verify implementation of corrective actions through testing, evidence upload, status tracking and linkage to risks, audit action plans and audit committee resolutions. Deliver dashboards and reporting to monitor implementation progress, recurring findings and governance oversight, supported by secure document management, audit-trail tracking and long-term archiving.

Perform ongoing internal and periodic external Quality Assurance

- Enable planning, scheduling and management of internal and external quality assurance reviews of the Internal Audit function, including scope definition, resource allocation and approval workflows. Provide functionality to capture quality review findings, recommendations, improvement actions and supporting evidence, with linkage to internal audit methodologies, standards and improvement plans. Deliver dashboards and reporting to monitor implementation of quality assurance recommendations and compliance with professional standards, supported by secure document management, role-based access control and full audit-trail tracking.

Future considerations (1)

Key responsibilities include:

- System Compliance and Governance: Reviewing whether policies and procedures are aligned with *m*SCOA requirements, ensuring proper change management and IT system maintenance, and verifying contract management for financial systems.
- Data Integrity and Validation: Providing assurance on the accuracy, completeness, and validity of data strings. Ensuring the municipality is fully transacting, not just reporting, on the integrated municipal system solution. Evaluating whether the integrated municipal system solution enables full compliance with the seven *m*SCOA segments.
- Risk Management and Controls: Evaluating the effectiveness of controls in the new business processes to mitigate risks. Assisting in enhancing accountability by auditing, reporting, and recommending improvements to internal controls.
- Proactive and Continuous Audit: Acting as an "early warning system" by performing ongoing risk assessments and audits.
- Performance and Technical Reviews: Assessing the integration of IT systems, data migration quality (assessing the accuracy of data cleaning and migration), and the overall functionality of the integrated municipal system solution.

Future considerations (2)

Internal Audit considerations in terms of the minimum business processes and systems specifications?

- Embedding technological advances, expanding the scope of services, investing in resource development, and enhancing advisory services.
- Evolving risks and topical requirements (GIAS): Cybersecurity, Environmental, Social and Governance (ESG), and Artificial Intelligence (AI), with the use of technology-based tools.
- IT systems are evolving from siloed on-premises solutions to interconnected cloud-based systems or hybrid systems, enabling greater scalability, flexibility and real-time data processing. IT systems must be faster, more effective and be resilient. *m*SCOA is the fundamental enabler for digital transformation. A standardised chart of accounts and uniform standard classification of data, including Business Processes (and minimum requirements). Effective audit of IT systems will add value to municipalities and municipal entities and is a continuous process.

Future considerations (3)

Internal Audit considerations in terms of the minimum business processes and systems specifications?

As AI-driven decision-making becomes more prevalent, municipalities and municipal entities need to ensure ethical accountability in automated systems (The responsibility for the preparation and review of the algorithmic outputs). In the simplest terms, data governance is about managing data as a strategic asset. It involves ensuring that there are controls in place around data, its content, structure, use, and safety.

- The concept of "risk" itself will evolve in response to advances in predictive analytics and AI, with the use advanced analytics tools (business intelligence analytics via Power BI Tools, identify trends and anomalies), exception reporting, dashboards, etc. to monitor real-time performance. Reduce errors in real-time auditing to improve accuracy with the early detection of issues, and increase control effectiveness.
- Combined audit assurance: Enhancing assurance via technology with integrated approaches, frameworks (compliance with the applicable legislation and standards) and King Report considerations.

Future considerations (4)

- Regular communication between assurance providers ensures alignment of plans, sharing of findings, and efficient use of resources
- Use of integrated system solutions provide a single, reliable data source for all assurance providers
- It is vital to align internal audit, risk management and external audit efforts
- This will enhance coordination and coverage of key risks
- The implementation of *mSCOA* business processes is not just a compliance exercise; it is a strategic tool for enhancing assurance. By improving data quality, strengthening controls, enabling real-time reporting, and supporting integrated assurance, *mSCOA* helps public institutions achieve higher levels of efficiency, accountability, and performance

Documentation on minimum business process and technical system specifications requirements (1)

Link to one drive: [G1_Draft Regulations - Training]

Name ↑	Modified
1_Regulations	November 22, 2...
10_Recordings_Dec 2025 ICF	February 1
11_Task Team Meetings	February 10
2_Position Papers	November 22, 2...
3_System Comments Registers - Dec 2025	December 12, 2...
4_Process Documents	November 18, 2...

Documentation on minimum business process and technical system specifications requirements (2)

Link to one drive: G1_Draft Regulations - Training

5_System Requirement Documents	November 18, 2...
6_Process Comments Registers - Dec 2025	December 11, 2...
7_System Comments Registers - Feb 2026	January 27
8_Process Comments Registers - Feb 2026	January 27
9_Regulations_Position Papers Comments Registers - Feb 2026	January 30