

## TERMS OF REFERENCE

### THE INFORMATION TECHNOLOGY (IT) GOVERNANCE COMMITTEE

---

*Ref: 426091*

#### 1. PURPOSE

Communicate the primary responsibilities and delegated authority of the IT Governance Committee for the oversight and monitoring of IT resources to facilitate the achievement of corporate objectives.

#### 2. ROLE OF THE SAICA BOARD

2.1. In terms of the third report on corporate governance (King III) the SAICA Board retains overall accountability for IT governance and, as such:

- Must ensure that IT is aligned with the performance and sustainability objectives of the company.
- Should require from management the implementation of an IT governance framework, including relevant charters, policies, procedures, standards and appropriate governance mechanisms.
- Should monitor and evaluate significant IT investments and expenditure.
- Should ensure that IT is given due consideration within SAICA's risk management process.
- Should ensure that information assets are adequately protected and managed effectively.
- Should require regular reporting from management on IT performance.

2.2. In terms of international standard on corporate governance of information technology (ISO/IEC 38500:2008), the Board should govern IT through three main tasks:

- Evaluate the current and future use of IT.
- Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.
- Monitor conformance to policies and performance against plans.

#### 3. ROLE OF THE IT GOVERNANCE COMMITTEE

The IT Governance Committee is formed to assist the Board in discharging its responsibilities listed above and, as such, is required to monitor the activities of the IT function against the provisions of the IT Charter and IT Governance framework and report on any shortcomings noted together with recommendations for their remediation.

#### 4. SCOPE / JURISDICTION OF THE IT GOVERNANCE COMMITTEE

4.1. The IT Governance Committee will focus on the strategic matters as these relate to IT Governance and will not be involved in operational issues. Therefore, the committee's scope of authority is limited to:

- Assisting the Board in its tasks of evaluation and monitoring of the IT function
- Considering IT compliance as it relates to business goals
- Ensuring that committee business does not focus on technical details but instead considers matters such as resource investment and allocation
- Taking a holistic view of the organisation and its systems architecture, including external service providers.
- Developing an understanding of the underlying dynamics that govern changes in technology and how such changes have the potential to alter SAICA's economic outlook and balancing the organisation's short-term business needs with long-term IT investments.
- Review and comment on the execution of SAICA's technology roadmap, ensuring that it is integrated within SAICA's strategic and business processes.
- Review and approve the IM Security Strategy as and when required.

4.2. The IT Governance Committee is therefore appointed in an advisory and review capacity to provide insight and advice to the Board. It does not have authority to approve or direct the acquisition or deployment of IT resources across the organisation.

4.3. The ambit of responsibility extends to SAICA and all its associated companies.

#### 5. IT GOVERNANCE COMMITTEE RESPONSIBILITIES AND FUNCTIONS

The IT Governance Committee's primary responsibilities include:

##### **Structure, relationships, frameworks and processes**

- 5.1. Ensure that an IT charter and policies are established and implemented by management.
- 5.2. To assess the IT governance and IT process and control frameworks and to require assurance over the IT governance mechanisms implemented by management.
- 5.3. Advise and comment on specific IT policies, on request.

##### **Strategic Alignment**

- 5.4. To serve as a sounding board for SAICA management and the SAICA Board in ensuring the effectiveness and efficiency of SAICA's information systems from a risk and strategic alignment perspective.

5.5. Review and comment on information management strategy in order to ensure that the IM strategy is aligned with the overall SAICA strategy. Specifically:

- To ensure that all initiatives are appropriate when considered in light of SAICA's overall strategic and business objectives
- To interrogate whether there is anything further IM could be doing to contribute to the achievement of SAICA's overall strategy and to improve performance and sustainability of the company in line with triple bottom line objectives
- To consider whether appropriate mechanisms are in place to adapt the IM strategy to changes in circumstances or changes in the SAICA strategy

5.6. To monitor the execution of the IM strategy. Specifically considering:

- Whether responsibility and accountability are clearly established
- Whether sufficient and appropriate resources are committed in accordance with priorities
- Whether tracking and monitoring mechanisms are in place

#### **Value Delivery**

5.7. To review and comment on the adequacy and necessity of the IT budget (fit for purpose) as planned over a one-year period and over a three-year period.

5.8. To ensure that a process exists and is consistently applied for prioritising and deciding on IT investments

5.9. To monitor significant IT investments and expenditure for expected benefit and delivery of value.

5.10. To require evidence of and provide assurance on request by the SAICA Board, Audit and Risk Committee and Finance Committee that due process has been followed by management in the consideration of any IT spend over and above the approved budget.

#### **Resource Management**

5.11. To assess whether SAICA has a well coordinated, efficient, effective and properly resourced IT function directed at enabling the organisation to effectively meet member expectations.

5.12. To review independent assurance of the effectiveness of the IT controls framework implemented by service providers

5.13. To ensure that information assets are protected. Specifically:

- To ensure that risks are understood from a business perspective
- To ensure that appropriate resources are devoted to treating risks
- To ensure that priorities in terms of risk management are clearly understood
- To ensure that key exposures are adequately addressed

## **Risk Management**

- 5.14. To evaluate whether IT risk has been appropriately considered and incorporated into the overall SAICA risk management processes.
- 5.15. To report to the Board any issues relating to the management of IT risk that may come to their attention, and to recommend mitigating actions.

## **Performance Reporting**

- 5.16. Review and comment on the IT scorecard, to review the results of such reporting and to escalate any issues to the Board.
- 5.17. Require reports from IT management and independent assurance providers, where appropriate, to obtain assurance over the following matters:
  - The adequacy of management's business resilience arrangements in place for disaster recovery
  - Compliance with IT laws and IT related rules, codes and standards are considered
  - Protection of management information, which should include information security, information management and information privacy

## **6. COMPOSITION AND APPOINTMENT OF THE IT GOVERNANCE COMMITTEE**

- 6.1. The composition of the committee shall be considered by the Nominations Committee and recommended for approval to the SAICA Board.
- 6.2. The chairman of the committee, and/or his duly appointed representative, shall report to the Board and any other SAICA governance body (upon request), on matters dealt with within the ambit of the committee's area of responsibility.
- 6.3. Membership of the committee shall comprise:
  - 6.3.1. Two (2) board representatives
  - 6.3.2. One (1) finance committee representative
  - 6.3.3. One (1) audit and risk committee representative
  - 6.3.4. SAICA's Chief Executive Officer or duly appointed alternate
  - 6.3.5. At least two (2) other non-executive members who are specialists in the field of IT, including but not limited to those employed by audit representatives.
  - 6.3.6. Invitees may be invited to the meeting by the Chief Executive Officer and may include:
    - Chief Information Officer
    - Senior Executive: Corporate Services
    - Board representatives
    - Any other person

## **7. RELATIONSHIPS**

- 7.1. The committee will report to the SAICA Board.
- 7.2. The committee will also have a dotted reporting line to the Audit and Risk Committee through the chairman of same.
- 7.3. The committee may also liaise closely with other senior SAICA personnel where necessary.

## **8. MEETINGS OF THE COMMITTEE**

The committee shall meet as often as is necessary for the effective performance of its duties but at least once a quarter. If a committee member is absent without apology and/or a valid reason for two (2) consecutive Information Technology Governance Committee meetings, membership of the committee may be forfeited.

## **9. QUORUM**

- 9.1. A quorum for a meeting of the committee shall be at least one non-executive board representative, the Chief Executive Officer or any member of Manco, other than the Chief Information Officer, appointed by the Chief Executive Officer and one non-executive specialist.
- 9.2. A duly convened meeting of the committee at which a quorum is present shall be competent to exercise all, or any, of the authorities, powers and discretions vested in or exercisable by the committee.

## **10. DELEGATION OF AUTHORITY**

Authority delegated to the IT Governance Committee is founded on the following principles:

- 10.1. Does not divest the Board of their responsibilities concerning the exercise of the delegated power or the performance of the assigned duties herein.
- 10.2. Is given to a committee whose membership integrates both IT and business knowledge.
- 10.3. Is subject to the statutory and legal limitations, recorded herein, and such other lawful limitations as may be applicable to the organisation from time to time.
- 10.4. Is subject to any limitations, conditions, policies and/or directives that may be developed and implemented by executive management at the request of the Board in the exercise of such delegated powers.
- 10.5. May at any time be revoked or varied by the Chief Executive Officer.
- 10.6. The Board may confirm, vary or revoke any decision taken by the IT Governance Committee as a result of a delegation in terms hereof, subject to any rights that may have become vested as a consequence of the decision.

10.7. Unless otherwise specified, the IT Governance Committee is hereby authorised, in writing, and subject to paragraphs 1 to 6 above to delegate further any powers and authority delegated to the IT Governance Committee to an officer, employee, any person or committee, in terms of the needs of the business, subject to the policies, directives and conditions that the Board may from time to time prescribe, and the reporting of such authority.

10.8. The IT Governance Committee or any other person with delegated powers may only exercise those powers in respect of the responsibilities and functions allocated to them from time to time, in terms of a performance agreement or specific instructions or mandates.

10.9. Reporting is to follow the delegation process i.e. any approvals need to be reported to the next level of authority. Non-conformance with the delegated powers shall be reported to the next higher level of authority.

#### **11. APPROVAL OF THESE TERMS OF REFERENCE**

These terms of reference as set out above were approved by the IT Governance Committee on 26 May 2010 with the understanding that this is a living document.

*Approved by IT Governance Committee on 14 March 2013*

*Approved by the Board on 25 April 2013*

*Noted by Audit & Risk Committee on 31 July 2013*