

Internal Audit Planning Checklist

A practical guide to preparing a focused, risk-based internal audit plan that connects assurance work to organisational objectives, key risks and available resources. Suitable for private, public and non-profit organisations.

Version 2.0 | October 2026

Designed for use alongside the Global Internal Audit Standards (effective 9 January 2025).

Organisation	
Planning period	
Prepared by	
Reviewed by (CAE / audit lead)	
Date	

How to use this checklist

Use the questions to guide annual or periodic audit planning. For each item, select a status, name the person responsible with a target date, and record the evidence reviewed or the decision made. The checklist supports professional judgement; it does not replace the organisation's risk assessment, audit charter, methodology or applicable legal and professional requirements.

Status	Meaning	Use when
C	Complete	The question is answered and the supporting evidence is on file.
PC	Partly complete	Work has started but evidence or coverage is incomplete. State what is outstanding.
A	Action required	The item has not been done or the answer is no. Name an owner and a date.
NA	Not applicable	The item does not apply. Record the reason, because a bare NA is not evidence.
★	Critical item	A shaded reference cell marks a critical item. These should not be closed by assertion alone.

Worked example

Ref	Planning question	Status	Owner / date	Evidence / notes / action
4.6	★ Have process owners and relevant managers been consulted to validate completeness and current ownership?	PC	Head of IA, 15 Nov	Universe v3 (12 Oct). Four of seven divisions confirmed. Finance and Procurement outstanding.

Good practice when completing it

- Record evidence, not assertions: cite the document, its version and its date.
- Where an item does not apply, say why. Where the answer is no, say what you will do about it.
- Complete the sector module in Appendix C that fits your organisation, if any.
- Adapt the checklist to the organisation's size, mandate, sector, risk profile and maturity. Public bodies should apply the legislation and public finance requirements of their own jurisdiction; private organisations and NGOs should apply their relevant governance, regulatory, donor and contractual obligations.

Ten-minute planning health check

Use this first to see where your planning process is strong and where it needs attention. Then work through the full checklist, starting with the sections you marked Partly or No.

#	Statement	Yes / Partly / No	Full checklist section
1	A board-approved charter is in place and internal audit's independence has been confirmed.		1
2	The audit universe has been validated with process owners within the last 12 months.		4
3	Risk ratings are documented, evidence-based and applied consistently.		5
4	Each planned engagement can be traced from objectives to risks to the engagement.		5, 7
5	Prior findings and other assurance providers have been considered, and any reliance is justified.		6
6	Capacity has been calculated after non-audit time, with contingency reserved.		9
7	High risks not covered by the plan are disclosed to the board with the potential consequence.		10, 11
8	IT, cyber, data and AI risks have been considered in the plan.		8
9	The board has approved the plan, and the resource implications are recorded.		12
10	Triggers and a process exist for revising the plan during the year.		13

Reading your result

- 9–10 Yes: a strong foundation. Use the full checklist to test the evidence behind each answer.
- 6–8 Yes: a workable process with gaps. Prioritise the sections linked to your Partly and No answers.
- 5 or fewer Yes: significant planning risk. Treat the plan as provisional and tell the approving body what is missing.

This is a self-assessment to start the conversation. It is not an assurance opinion.

1. Confirm mandate, independence and charter

Planning starts with authority and objectivity. A plan prepared by a team with unmanaged impairments, or without a current mandate, is difficult to defend however good the risk analysis.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
1.1	★ Is there a current internal audit charter approved by the board (or equivalent governing body), and has it been reviewed within the agreed cycle?			
1.2	★ Does the charter define purpose, authority, responsibilities, reporting lines and unrestricted access to records, people, systems and locations?			
1.3	★ Has the chief audit executive (CAE) or internal audit lead confirmed organisational independence, including a functional reporting line to the board or audit committee?			
1.4	★ Have planning team members declared conflicts of interest, and have impairments to objectivity (for example, recent management responsibility for, or advisory work on, an area proposed for audit) been identified and managed under the methodology?			
1.5	Is the scope of the internal audit function clear, including any areas excluded from its mandate?			
1.6	Where internal audit holds non-audit responsibilities (for example, risk management, compliance or management of other functions), have safeguards been agreed and disclosed to the board?			
1.7	Are the approved methodology, quality standards and reporting expectations available to everyone involved in planning?			

2. Understand the organisation and its objectives

Start with the organisation's purpose, operating environment and the changes that could affect delivery of its strategy.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
2.1	★ Have the organisation's mandate, strategy, objectives and key performance commitments been reviewed?			
2.2	Have material changes in leadership, structure, systems, services, funding or operating model been identified?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
2.3	Have external factors such as economic conditions, regulation, technology, cyber threats, suppliers, geopolitical developments and stakeholder expectations been considered?			
2.4	Have prior-period performance reports, management reports, financial results and relevant external assessments been reviewed?			
2.5	Have significant incidents, complaints, fraud allegations, litigation, service failures or business interruptions been considered?			
2.6	★ Have the expectations of the board, audit committee, executive management and other key stakeholders been obtained and recorded?			
2.7	Has the maturity of governance, risk management and internal control processes been assessed, so that audit effort reflects what is already working and what is not?			
2.8	Have organisational culture, ethics and speak-up arrangements been considered as inputs to risk?			

3. Set the internal audit strategy and map assurance

The annual plan should follow from a strategy, not replace one. An assurance map shows where internal audit adds most value and where other providers already give reliable comfort.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
3.1	★ Is there an internal audit strategy (typically multi-year) that links to the organisation's strategy and the board's expectations, and has it been reviewed this cycle?			
3.2	Does the strategy state the function's objectives and how its performance will be measured?			
3.3	Has an assurance map been prepared or updated, showing assurance across management, risk and compliance functions, internal audit and external providers?			
3.4	Are overlaps and gaps in assurance identified, and do they inform where internal audit effort is directed?			
3.5	Is the planned mix of assurance, advisory, follow-up, investigations and data-analytics work consistent with the strategy?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
3.6	Has the planning approach (annual, rolling with periodic refresh, or hybrid) been chosen and the reason recorded?			
3.7	Has the CAE considered whether planned coverage will be sufficient to support the overall conclusion the board expects from internal audit?			

4. Build and validate the audit universe

The audit universe should give a sufficiently complete, current and traceable view of the areas that may warrant assurance or advisory work.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
4.1	★ Does the audit universe cover key business units, programmes, functions, locations, systems, major projects and outsourced services?			
4.2	Are material financial, operational, compliance, governance, technology, data and strategic processes represented?			
4.3	Have procurement and contract management, revenue, payroll, assets, grants and other high-risk processes been considered where relevant?			
4.4	Have significant third parties, shared services, joint ventures, implementing partners or service providers been included where the organisation relies on them?			
4.5	Have new or emerging activities been added, and discontinued activities removed, since the previous planning cycle?			
4.6	★ Have process owners and relevant managers been consulted to validate completeness and current ownership?			
4.7	Is each auditable entity mapped to organisational objectives and to the risks it addresses, so that coverage can be traced?			
4.8	Is the universe version-controlled and dated, and maintained as a living record rather than rebuilt each year?			

Next step: capture and score your universe in a structured workbook. The Muzamani Audit Universe Builder (Excel) is designed to support this step. Visit muzamani.com.

5. Assess and prioritise risks

Document how risks were identified, assessed and ranked. Use the organisation's approved risk methodology where one exists; Appendix A offers a simple fallback.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
5.1	★ Have the latest enterprise risk register and relevant operational, project, IT, fraud and compliance risk assessments been reviewed?			
5.2	If no reliable risk register exists, has internal audit's own risk assessment been documented and the limitation reported to the board?			
5.3	★ Have inherent risk, existing controls and residual risk been distinguished clearly?			
5.4	★ Are likelihood and impact ratings supported by evidence and applied consistently using a documented scale?			
5.5	Have financial, service delivery, safety, legal, regulatory, reputational, cyber, privacy, environmental, social and strategic impacts been considered as applicable?			
5.6	Have fraud, corruption, conflicts of interest, procurement abuse and management override risks been considered?			
5.7	Have emerging risks, repeat incidents, control failures and overdue high-risk actions been considered?			
5.8	Have operational resilience, third-party concentration, key-person dependency and ethics and culture risks been considered?			
5.9	Where stakeholder requests or known assurance gaps changed the risk-based ranking, is each override documented with who requested it, why and who approved it?			
5.10	★ Is the rationale for the highest-ranked risks recorded and capable of being explained to the audit committee?			

6. Review prior assurance and outstanding actions

Use existing assurance work to avoid unnecessary duplication and to identify where additional assurance is needed.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
6.1	★ Have previous internal audit reports and outstanding recommendations been reviewed, including overdue high-risk actions?			
6.2	Have external audit findings and relevant regulator, inspectorate, donor or certification reviews been considered?			
6.3	Have risk management, compliance, quality assurance, security, health and safety and other assurance results been considered?			
6.4	Have recurring findings and root causes been identified, rather than treating each finding as an isolated issue?			
6.5	Has reliance on other assurance providers been assessed for competence, objectivity, scope, quality and currency of their work?			
6.6	Are areas with limited or no reliable assurance identified?			
6.7	Is follow-up of previous actions planned and resourced, and are risks that management has accepted identified for the board?			

7. Select audit engagements and define coverage

Convert risk priorities into a balanced set of proposed engagements. Explain why each engagement is included, deferred or excluded.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
7.1	★ Does each proposed engagement link to a material risk, organisational objective, control concern or stakeholder need?			
7.2	Is the objective of each engagement clear and focused on the assurance or advisory question to be answered?			
7.3	Is the proposed scope proportionate to the risk and specific enough to guide fieldwork?			
7.4	Are the timing, frequency and coverage of recurring audits justified by risk rather than habit?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
7.5	Have mandatory, regulatory, contractual, donor or audit committee commitments been identified?			
7.6	Have cross-cutting themes such as procurement and supply chain, information security, data governance, fraud risk, change projects and third-party management been considered?			
7.7	Have advisory requests been distinguished from independent assurance engagements, with safeguards for objectivity where advisory work is accepted?			
7.8	★ Are proposed exclusions, deferrals and accepted coverage gaps documented with reasons?			
7.9	Has time been planned for follow-up, investigations, management requests and data analytics or continuous auditing, where these form part of the strategy?			

8. Consider IT, data and emerging technology risks

Include technology and information risks in the plan wherever they affect key processes, services or reporting. Appendix D lists common reference frameworks.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
8.1	★ Have critical systems, interfaces, access rights, change management, IT operations and system availability been considered?			
8.2	Have cybersecurity, privacy, data integrity, backup and recovery risks been considered where relevant?			
8.3	Have significant technology implementations, migrations, cloud services and outsourced IT arrangements been considered?			
8.4	Have identity and privileged access management, logging and monitoring, and incident response arrangements been considered?			
8.5	Have risks from software vendors, managed service providers and other technology suppliers been considered?			
8.6	Have automated controls, spreadsheets and other end-user computing, data quality and reliance on system-generated reports been considered?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
8.7	★ Where AI is used or being introduced, have governance, data confidentiality, output validation, access, accountability and vendor risks been considered?			
8.8	Is the use of AI within internal audit itself governed, including confidentiality of audit evidence, validation of AI output and professional accountability for conclusions?			
8.9	Have IT audit skills, specialist support and data analytics needs been identified?			
8.10	Where a framework such as COBIT, ISO/IEC 27001 or the NIST Cybersecurity Framework is in use, is planned coverage aligned to its scope?			

9. Confirm capacity, skills and budget

A risk-based plan must be realistic about the people, time, budget and specialist skills available. Appendix B provides a capacity worksheet.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
9.1	★ Have available audit days been calculated after leave, administration, training, quality activities and other non-audit commitments?			
9.2	Have engagement days been estimated using complexity, risk, geographic spread, expected evidence requirements and actual effort on comparable past engagements?			
9.3	Are the required skills available in areas such as finance, procurement, IT, cyber, data analytics, investigations and sector regulation?			
9.4	Have co-sourcing, specialist support or external expertise needs been identified and costed where possible?			
9.5	★ Does the proposed plan fit the approved budget and reporting timetable, and if not, has the shortfall been quantified for the board?			
9.6	Have contingency days been reserved for urgent requests, investigations and material emerging risks?			
9.7	Have time and budget been included for quality assurance and improvement activities and for staff development?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
9.8	Have competing priorities and capacity constraints been made visible to decision-makers?			

Next step: turn this section into a working capacity model. The Muzamani Internal Audit Toolkit Lite includes planning templates for this purpose. Visit muzamani.com.

10. Prepare the draft plan

The draft should make priorities, timing, resources and the consequences of constraints clear to those who will approve it.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
10.1	★ Does the draft plan list each engagement with its objective, risk rationale, proposed scope and indicative timing?			
10.2	Does it identify the responsible audit lead, estimated effort and specialist requirements where known?			
10.3	Does it show how high-risk areas, mandatory work and stakeholder priorities will be covered?			
10.4	★ Are material risks not covered by the plan clearly disclosed, with the reason and the potential consequence?			
10.5	Have management views been obtained without compromising internal audit independence, and are any management-requested changes recorded?			
10.6	Has the CAE or internal audit lead reviewed the plan for completeness, feasibility and alignment with the charter and strategy?			
10.7	Does the plan explain how progress will be reported and how it can be changed during the year?			

11. Pre-submission readiness gate

Complete this gate before the plan goes to the board or audit committee. Every item should be Complete, or Not applicable with a recorded reason, before submission.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
11.1	★ The audit universe is sufficiently complete and has been validated.			
11.2	★ The prioritisation of engagements is based on documented risk and professional judgement.			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
11.3	★ Prior audit findings and other assurance work have been considered.			
11.4	★ The proposed plan is feasible with the available skills, time and budget, or the constraints are disclosed.			
11.5	★ High-risk areas not covered by the plan are clearly identified and explained.			
11.6	★ No unresolved conflicts of interest or impairments to objectivity affect the planning team or the proposed engagements.			
11.7	Stakeholder input has been considered while internal audit independence is preserved.			
11.8	The draft plan includes clear engagement objectives, indicative timing and resource estimates.			
11.9	The plan carries a version number, date and author, and is ready for submission.			

12. Approval, communication and record

Complete this section after submission. The record should show what was approved, by whom, on what basis and with what limitations.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
12.1	★ Has the plan been submitted to the board, audit committee or equivalent governing body for review and approval?			
12.2	★ Has the impact of any resource limitations been communicated to the governing body and recorded?			
12.3	★ Are the approval, version, date, any conditions and the minute or decision reference recorded?			
12.4	Has the approved plan been communicated to management and process owners as appropriate, while protecting the confidentiality of sensitive engagements?			
12.5	Have changes requested by the governing body been documented and reflected in a revised version of the plan?			

13. Monitor delivery and update the plan

Planning is not a once-a-year exercise. The plan should respond to significant changes in risk and delivery.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
13.1	Is there a process for monitoring engagement delivery, time spent, budget and changes in scope?			
13.2	Are delays, cancellations, resource constraints and emerging coverage gaps reported to the appropriate level?			
13.3	★ Are triggers for revising the plan defined, such as a major incident, material fraud, new regulation, system failure or significant organisational change?			
13.4	Are proposed changes to the plan risk-assessed, documented and approved at the appropriate level?			
13.5	Is progress against the plan reported periodically to the audit committee or governing body?			
13.6	Are the performance measures set in the internal audit strategy (for example, plan completion, follow-up closure and stakeholder feedback) tracked?			
13.7	Are lessons from completed engagements and changes in the risk profile fed into the next planning cycle?			

Planning summary and readiness assessment

Readiness tally

Status	Critical (★) items, Sections 1–11	All items, Sections 1–13
Complete (C)		
Partly complete (PC)		
Action required (A)		
Not applicable (NA)		
Total items	28	102

Readiness decision

Ready to submit	Every critical item in Sections 1–11 is Complete, or Not applicable with a recorded reason.
Submit with disclosed limitations	Some critical items are Partly complete, and each limitation is stated in the plan and communicated to the approving body.
Not ready	Any critical item in Sections 1–11 is marked Action required. Resolve it, or escalate the constraint before submission.

Planning summary

Plan version and date	
Number of engagements proposed	
Highest-priority risks addressed	
Material risks not covered, with reasons and consequence	
Resource or skills gaps	
Net available audit days / days required	
Approval body and approval date	
Next planned review date	

Appendix A: Risk rating guide (optional)

Use the organisation's approved risk methodology where one exists. Where there is none, this simple scale gives a documented and repeatable starting point. Adapt the descriptors to the organisation's own context and risk appetite.

Likelihood ↓ Impact →	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Band	Score	Suggested planning response
Low	1–4	Monitor. Consider advisory work or reliance on other assurance.
Medium	5–9	Cover on a rotational basis, or rely on other assurance if it has been assessed as reliable.
High	10–16	Priority for coverage within the plan period.
Critical	20–25	Include in the plan. If not covered, disclose to the board with the reason and consequence.

Score = likelihood × impact. Rate residual risk after considering existing controls, and record the evidence behind each rating.

Override rule: any engagement added, removed or re-ranked against the scoring outcome should record who requested the change, the reason and who approved it.

Appendix B: Audit capacity worksheet

Complete this before confirming Section 9. Use days or hours consistently, and state the planning period.

Line	Item	How to calculate	Days
A	Number of internal audit staff (full-time equivalents)	Enter	
B	Gross working days per person in the period	Enter, after weekends	
C	Gross available days	$A \times B$	
D	Less: leave and public holidays	Enter	
E	Less: training and professional development	Enter	
F	Less: administration, meetings and management	Enter	
G	Less: quality assurance and improvement activities	Enter	
H	Less: other non-audit commitments	Enter	
I	Net available audit days	$C - D - E - F - G - H$	
J	Contingency (urgent requests, investigations, emerging risks)	CAE to set and justify	
K	Follow-up and recurring monitoring	Enter	
L	Days available for planned engagements	$I - J - K$	
M	Days required by proposed engagements	Sum of engagement estimates	
N	Surplus / (shortfall)	$L - M$. Disclose any shortfall to the approving body.	

Appendix C: Sector modules

Complete the module that fits the organisation, in addition to Sections 1–13. Modules can be combined, for example for a public entity that receives donor funding.

Public sector module

For government departments, municipalities, public entities and state-owned enterprises. Identify the legislation and treasury requirements of your own jurisdiction; South African examples are given for illustration.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
P.1	★ Have the public finance management legislation, treasury regulations or instructions and internal audit requirements of the jurisdiction been identified and reflected in the plan (for example, the PFMA or MFMA in South Africa)?			
P.2	Does the plan meet any statutory requirements for internal audit and audit committee coverage, frequency and reporting?			
P.3	★ Have procurement and supply chain probity risks been covered based on risk: competitive bidding, deviations, contract variations and extensions, declarations of interest, delegations of authority and segregation of duties?			
P.4	Have irregular, unauthorised, and fruitless and wasteful expenditure (or equivalent categories) and consequence management been considered?			
P.5	Have findings of the auditor-general or supreme audit institution been analysed, and are repeat findings tracked?			
P.6	Has the reliability of performance information and reporting against predetermined objectives been considered?			
P.7	Have transfers, grants, public-private arrangements and entities under the organisation's oversight been considered?			

NGO and donor-funded module

For non-profit organisations, foundations and programmes funded by donors or grants.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
N.1	★ Have donor agreements, grant conditions and reporting requirements been reviewed for audit rights, access and fraud-reporting obligations?			
N.2	Have restricted funds, cost allocation and allowable-cost compliance been considered?			

Ref	Planning question	Status	Owner / date	Evidence / notes / action
N.3	★ Have sub-grantee and implementing-partner due diligence and monitoring been considered?			
N.4	Have safeguarding, protection from sexual exploitation, abuse and harassment, and whistleblowing arrangements been considered?			
N.5	Have field offices, cash handling, remote or high-risk locations and access constraints been considered?			
N.6	Has the reliability of programme results and beneficiary data been considered?			
N.7	Have diversion and fraud risks in programme supply chains, and sanctions and counter-terrorism financing obligations, been considered?			

Private and regulated sector module

For listed, privately held and regulated commercial organisations.

Ref	Planning question	Status	Owner / date	Evidence / notes / action
R.1	★ Have applicable regulatory, licensing, listing and sector-specific requirements been identified and covered (for example, financial services, healthcare or utilities)?			
R.2	Have corporate governance code and listing-rule expectations for internal audit, risk management and internal control reporting been considered?			
R.3	Where applicable, have internal control over financial reporting requirements (for example, SOX in the United States) and reliance by external auditors been considered?			
R.4	Have revenue assurance, pricing, commercial contracts, customer credit exposure and acquisition integration been considered?			
R.5	Have group structure, subsidiaries, joint ventures, intercompany arrangements and foreign operations been considered?			
R.6	Have sustainability and ESG reporting, and any assurance requirements over it, been considered?			
R.7	Have anti-bribery and corruption, sanctions and data protection obligations across the jurisdictions of operation been considered?			

Appendix D: Standards and framework references

The table shows where each section aligns with the Global Internal Audit Standards (GIAS) and other widely used frameworks. It is provided for orientation. Clause references reflect the 2024 Standards structure; verify them against the published Standards before quoting them in an engagement or plan.

Checklist section	Principal GIAS alignment	Supporting references
1. Mandate, independence and charter	GIAS Principles 2, 6 and 7 (including Standards 2.1–2.3, 6.1, 6.2 and 7.1)	Organisation's own charter and methodology
2. Understand the organisation	GIAS Standard 9.1	COSO Internal Control – Integrated Framework (2013)
3. Strategy and assurance map	GIAS Standards 9.2, 9.3 and 9.5	IIA Three Lines Model (2020)
4. Audit universe	GIAS Standards 9.1 and 9.4	Organisation's objectives and risk register
5. Risk assessment and prioritisation	GIAS Standards 9.1 and 9.4	ISO 31000:2018; COSO ERM (2017)
6. Prior assurance and follow-up	GIAS Standards 9.5, 11.5 and 15.2	External audit, regulator and donor reports
7. Engagement selection and coverage	GIAS Standard 9.4	Charter, audit committee terms of reference
8. IT, data and emerging technology	GIAS Standards 9.4 and 10.3	COBIT 2019; ISO/IEC 27001:2022; NIST CSF 2.0; ISO/IEC 42001:2023; NIST AI RMF 1.0
9. Capacity, skills and budget	GIAS Principle 10 (Standards 10.1–10.3) and Standard 8.2	Quality assurance and improvement programme
10. Draft plan	GIAS Standard 9.4	Organisation's planning template
11. Pre-submission gate	GIAS Standards 2.2, 2.3 and 9.4	Internal quality review procedures
12. Approval and record	GIAS Standards 8.1, 8.2 and 9.4	Board and audit committee minutes
13. Monitoring and updates	GIAS Standards 9.4 and 12.2	Audit committee reporting calendar

Important professional note

This checklist is a general planning aid, not a substitute for professional judgement or organisation-specific requirements. Use it with the current Global Internal Audit Standards, the approved internal audit charter and methodology, and applicable laws, regulations and governance requirements. Adapt the content to the organisation's mandate, risk profile and resources.

References to the Global Internal Audit Standards and to other frameworks are for orientation only. The Standards are published by The Institute of Internal Auditors. This checklist does not reproduce them and is not endorsed by or affiliated with that institute.

Completing this checklist does not constitute an assurance opinion, and it does not guarantee compliance with any standard, law or regulation.

Muzamani Services (Pty) Ltd

Internal audit, IT audit, risk management, governance and compliance advisory

muzamani.com