

Glossary of terms, acronyms and abbreviations

Glossary of key terminology used in this report

<i>Adverse audit opinion (on financial statements)</i>	The financial statements contain misstatements (see ‘misstatement’) that are not confined to specific amounts, or the misstatements represent a substantial portion of the financial statements.
<i>Asset (in financial statements)</i>	Any item belonging to the auditee, including property, infrastructure, equipment, cash, and debt due to the auditee.
<i>Assurance / assurance provider</i>	<p>As used in this report, assurance is a positive declaration that is intended to give confidence in the credibility of financial and performance reports tabled by auditees and in the extent to which auditees have adhered to applicable legislation.</p> <p>Through the audit report issued to the auditees, we provide assurance on the credibility of auditees’ financial and performance information as well as their compliance with key legislation.</p> <p>There are role players in local government (assurance providers), other than the external auditors, that are also required to contribute to assurance and confidence by ensuring that adequate internal controls are implemented to achieve auditees’ financial, service delivery and compliance objectives. Such assurance providers include senior auditee officials, various committees (for example, municipal public accounts, performance and audit committees) and internal audit units.</p> <p>Other role players that should provide assurance further include oversight structures and coordinating or monitoring departments (see ‘oversight structures as well as coordinating and monitoring departments’).</p>
<i>Backups</i>	In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so that it may be used to restore the original after a data loss event. The primary purpose of a backup is to recover data after its loss, be it by data deletion or corruption.
<i>Business continuity plan (BCP)</i>	A business continuity plan is a plan to continue operations if a place of business is affected by different levels of disaster, which can be localised short-term disasters, to days-long building-wide problems, to a permanent loss of a building. Such a plan typically explains how the business would recover its operations or move operations to another location after damage by events like natural disasters, theft or flooding. For example, if a fire destroys an office building or data centre, the people and business or data centre operations would relocate to a recovery site.

<i>Capital budget</i>	The estimated amount planned to be spent by auditees on capital items in a particular financial period; for example, fixed assets such as property, infrastructure and equipment with long expected lives and that are required to provide services, produce income or support operations.
<i>Cash flow (in financial statements)</i>	The flow of money from operations: incoming funds are revenue (cash inflow) and outgoing funds are expenses (cash outflow).
<i>Clean audit</i>	The financial statements receive a financially unqualified audit opinion and there are no material findings on the quality of the annual performance report or compliance with key legislation.
<i>Commitments from role players</i>	Initiatives and courses of action communicated to us by role players in local government aimed at improving the audit outcomes.
<i>Conditional grants</i>	Money transferred from national government to auditees, subject to certain services being delivered or on compliance with specified requirements.
<i>Consolidated financial statements</i>	Financial statements that reflect the combined financial position and results of a municipality and those of the municipal entities under its control.
<i>Contingent liability</i>	A potential liability, the amount of which will depend on the outcome of a future event.
<i>Creditors</i>	Persons, companies or organisations that the auditee owes money to for goods and services procured from them.
<i>Current assets (in financial statements)</i>	These assets are made up of cash and other assets, such as inventory or debt for credit extended, which will be traded, used or converted into cash in less than 12 months. All other assets are classified as non-current, and typically include property, plant and equipment as well as long-term investments.
<i>Disaster recovery plan (DRP)</i>	A disaster recovery plan is a documented process or set of procedures to recover and protect an auditee's information technology infrastructure in the event of a disaster. Usually documented in written form, the plan specifies the procedures that an auditee should follow in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The disaster could be natural, environmental or artificial. Artificial disasters could be intentional, such as the act of an attacker; or unintentional (in other words, accidental), such as the wall of a dam breaking).

Disclaimed opinion (on financial statements)

The auditee provided insufficient evidence in the form of documentation on which we could base an audit opinion. The lack of sufficient evidence is not confined to specific amounts, or represents a substantial portion of the information contained in the financial statements.

Financial and performance management (as one of the drivers of internal control)

The performance of internal control and monitoring-related tasks by management and other employees to achieve the financial management, reporting and service delivery objectives of the auditee.

These controls include basic daily and monthly controls for processing and reconciling transactions, preparing regular and credible financial and performance reports as well as reviewing and monitoring compliance with key legislation.

Financially unqualified audit opinion (on financial statements)

The financial statements contain no material misstatements (see 'material misstatement'). Unless we express a clean audit opinion, findings have been raised on either the annual performance report or compliance with key legislation, or both these aspects.

196

Firewall

A security system used to prevent unauthorised access between networks (both internal/internal and internal/external). A firewall will allow only approved traffic in and/or out by filtering packets based on the source or destination. The firewall inspects the identification information associated with all communication attempts and compares it to a rule set consistent with the auditee's security policy. Its decision to accept or deny the communication is then recorded in an electronic log.

Fruitless and wasteful expenditure

Expenditure that was made in vain and could have been avoided had reasonable care been taken. This includes penalties and interest on the late payment of creditors or statutory obligations as well as payments for services not utilised or goods not received.

Going concern

The presumption that an auditee will continue to operate in the near future, and will not go out of business and liquidate its assets. For the going concern presumption to be reasonable, the auditee must have the capacity and prospect to raise enough financial resources to stay operational.

Governance (as one of the drivers of internal control)

The governance structures (audit committees) and processes (internal audit and risk management) of an auditee.

Human resource (HR) management

The management of an auditee's employees, or human resources, which involves adequate and sufficiently skilled people as well as the adequate management of their performance and productivity.

<i>Information technology (IT)</i>	The computer systems used for recording, processing and reporting financial and non-financial transactions.
<i>IT controls</i>	Computer-related controls ensure the confidentiality, integrity and availability of state information; enable service delivery; and promote national security.
<i>IT governance</i>	The leadership, organisational structures and processes which ensure that the auditee's information technology resources will sustain its business strategies and objectives.
<i>IT security management</i>	The controls preventing unauthorised access to the computer networks, computer operating systems and application systems that generate and prepare financial information.
<i>IT service continuity</i>	The processes of managing the availability of computer hardware, system software, application software (computer programmes) and data to enable auditees to recover or establish information system services in the event of a disaster.
<i>IT user access management</i>	The procedures through which auditees ensure that only valid and authorised users are allowed segregated access to initiate and approve transactions on the information systems.
<i>Internal control / key controls</i>	<p>The process designed and implemented by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of the auditee's objectives with regard to the reliability of financial reporting, the effectiveness and efficiency of operations, and compliance with key legislation.</p> <p>It consists of all the policies and procedures implemented by auditee management to assist in achieving the orderly and efficient conduct of business, including adhering to policies, safeguarding assets, preventing and detecting fraud and error, ensuring the accuracy and completeness of accounting records, and timeously preparing reliable financial and service delivery information.</p>
<i>Irregular expenditure</i>	Expenditure incurred without complying with applicable legislation.
<i>Key drivers of internal control</i>	The three components of internal control that should be addressed to improve audit outcomes, namely leadership, financial and performance management, and governance (which are defined elsewhere in this glossary.)

Leadership *(as one of the drivers of internal control)*

The administrative leaders of an auditee, such as municipal managers and senior management.

It can also refer to the political leadership (including the mayor and the council) or the leadership in the province (such as the premier).

Material finding *(from the audit)*

An audit finding on the quality of the annual performance report or compliance with key legislation that is significant enough in terms of either its amount or its nature, or both these aspects, to be reported in the audit report.

Material misstatement

(in financial statements or annual performance reports)

An error or omission that is significant enough to influence the opinions or decisions of users of the reported information. Materiality is considered in terms of either its rand value or the nature and cause of the misstatement, or both these aspects.

Misstatement *(in financial statements or annual performance reports)*

Incorrect or omitted information in the financial statements or annual performance report.

Net current liability

The amount by which the sum of all money owed by an auditee and due within one year exceeds the amounts due to the auditee within the same year.

Net deficit *(incurred by auditee)*

The amount by which an auditee's spending exceeds its income during a period or financial year.

Operational budget / operating budget

A short-term budget, usually prepared annually, based on estimates of income and expenses associated with the auditee's operations, such as service delivery costs, administration and salaries.

Oversight structures as well as coordinating and monitoring departments

Oversight structures consist of the provincial legislatures, the portfolio committees on local government and the National Council of Provinces.

Coordinating or monitoring departments include the Department of Performance Monitoring and Evaluation, the National Treasury and provincial treasuries, the national and provincial departments of cooperative governance as well as the offices of the premier.

Password

In access control, confidential authentication information, usually composed of a string of characters, may be used to control access to physical areas and data. Passwords have to comply with certain complexity rules to ensure that they are not easy to guess.

<i>Property, infrastructure and equipment (in financial statements)</i>	Assets that physically exist and are expected to be used for more than one year, including land, buildings, leasehold improvements, equipment, furniture, fixtures and vehicles.
<i>Qualified audit opinion (on financial statements)</i>	The financial statements contain material misstatements in specific amounts, or there is insufficient evidence for us to conclude that specific amounts included in the financial statements are not materially misstated.
<i>Receivables / debtors (in financial statements)</i>	Money owed to the auditee by persons, companies or organisations that have procured goods or services from the auditee.
<i>Reconciliation (of accounting records)</i>	The process of matching one set of data to another; for example, the bank statement to the cheque register, or the accounts payable journal to the general ledger.
<i>Root causes (of audit outcomes being poor or not improving)</i>	The underlying causes or drivers of audit findings; in other words, why the problem occurred. Addressing the root cause helps to ensure that the actions address the real issue, thus preventing or reducing the incidents of recurrence, rather than simply providing a one-time or short-term solution.
<i>Supply chain management (SCM)</i>	Procuring goods and services through a tender or quotation process and monitoring the quality and timeliness of the goods and services provided.
<i>Unauthorised expenditure</i>	Expenditure that was in excess of the amount budgeted or allocated by government to the auditee, or that was not incurred in accordance with the purpose for which it was intended.
<i>Vulnerability</i>	In information security, a weakness or flaw (in location, physical layout, organisation, management, procedures, personnel, hardware or software) that may be exploited by an attacker to cause an unfavourable impact.

Acronyms and abbreviations used in this report

AFS	<i>annual financial statements</i>
AG	<i>auditor-general (the person)</i>
AGSA	<i>Auditor-General of South Africa (the institution)</i>
APAC	<i>Association of Public Accounts Committees</i>
APP	<i>annual performance plan</i>
APR	<i>annual performance report</i>
BCP	<i>business continuity plan</i>
CBD	<i>central business district</i>
CEO	<i>chief executive officer</i>
CFO	<i>chief financial officer</i>
CGICTPF	<i>corporate governance of information and communications technology policy framework</i>
CoGTA	<i>Department of Cooperative Governance and Traditional Affairs</i>
DM	<i>district municipality</i>
DoRA	<i>Division of Revenue Act</i>
DPME	<i>Department of Performance Monitoring and Evaluation</i>
DRP	<i>disaster recovery plan</i>
EC	<i>Eastern Cape</i>
FMG	<i>financial management grant</i>
FS	<i>Free State</i>
GP	<i>Gauteng</i>
GRAP	<i>Generally Recognised Accounting Practice</i>
HR	<i>human resources</i>
ICDG	<i>integrated city development grant</i>
ICT	<i>information and communications technology</i>
IDP	<i>integrated development plan</i>
ISDG	<i>infrastructure skills development grant</i>
IT	<i>information technology</i>
KFA	<i>key focus area</i>
KPA	<i>key performance area</i>
KPI	<i>key performance indicator</i>
KZN	<i>KwaZulu-Natal</i>
LGMIM	<i>local government management improvement model</i>

LGTAS	<i>local government turnaround strategy</i>
LM	<i>local municipality</i>
LP	<i>Limpopo</i>
M/metro	<i>metropolitan municipality</i>
MASP	<i>municipal audit support programme</i>
MAT	<i>municipal assessment tool</i>
ME	<i>municipal entity</i>
MEC	<i>member of the executive council</i>
MFMA	<i>Municipal Finance Management Act, 2003 (Act No. 56 of 2003)</i>
MIG	<i>municipal infrastructure grant</i>
MISA	<i>Municipal Infrastructure Support Agent</i>
MP	<i>Mpumalanga</i>
MPAC	<i>municipal public accounts committee</i>
MSA	<i>Municipal Systems Act, 2000 (Act No. 32 of 2000)</i>
MSIG	<i>municipal systems improvement grant</i>
MTSF	<i>medium term strategic framework</i>
MUN	<i>municipality</i>
NC	<i>Northern Cape</i>
NCOP	<i>National Council of Provinces</i>
NDPG	<i>neighbourhood development partnership grant</i>
NW	<i>North West</i>
SALGA	<i>South African Local Government Association</i>
SCM	<i>supply chain management</i>
SDBIP	<i>service delivery and budget implementation plan</i>
WC	<i>Western Cape</i>

[This page is intentionally left blank.]