GLOSSARY OF TERMS, ACRONYMS AND ABBREVIATIONS

Glossary of key terminology used in this report

Adverse audit opinion (on financial statements)

The financial statements contain material misstatements (see ‘misstatement’) that are not confined to specific amounts, or the misstatements represent a substantial portion of the financial statements.

Asset (in financial statements)

Any item belonging to the auditee, including property, infrastructure, equipment, cash, and debt due to the auditee.

Assurance & assurance provider

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 legislation to which they are subject.

Through the audit report issued to auditees, we provide assurance on the credibility of auditees’ financial and performance information as well as auditees’ compliance with key legislation.

There are role players (‘assurance providers’) in national and provincial government, other than 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 (heads of departments, accounting officers, and chief executive officers), various committees (risk management and audit committees), and internal audit units.

Other role players further include national and provincial oversight structures and coordinating or monitoring departments, as discussed in this report.

Backups

In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. The verb form is to back up in two words, whereas the noun is a backup. The primary purpose of a backup is to recover data after its loss, be it by data deletion or corruption

Business continuity plan (BCP)

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.

Capital budget

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.

Cash flow (in financial statements)

The flow of money from operations: incoming funds are revenue (cash inflow) and outgoing funds are expenses (cash outflow).

Clean audit

The financial statements receive a financially unqualified audit opinion and there are no material findings on the quality of the annual performance report or non-compliance with key legislation.

Commitments from role players

Initiatives and courses of action communicated to us by role players in national and provincial government aimed at improving the audit outcomes.

Conditional grants

Money transferred from national government to auditees, subject to certain services being delivered or on compliance with specified requirements.

Configuration

The complete technical description required to build, test, accept, install, operate, maintain and support a system.

Contingent liability

A potential liability, the amount of which will depend on the outcome of a future event.

Creditors

Persons, companies or organisations that auditees owe money to for goods and services procured from them.

Current assets (in financial statements)

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.

Data integrity

Data integrity refers to the overall completeness, accuracy and consistency of data. This can be indicated by the absence of alteration between two instances or between two updates of a data record, meaning data is intact and unchanged.

Disaster recovery plan (DRP)

A disaster recovery plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Usually documented in written form, the plan specifies the procedures that an organisation is to 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 man-made. Man-made disasters could be intentional (e.g. the act of an attacker) or unintentional (i.e. accidental, such as the wall of a man-made dam breaking).

Disclaimed audit 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 tasks relating to internal control and monitoring by management and other employees to achieve the financial management, reporting and service delivery objectives of the auditee.

These controls include the basic daily and monthly controls for the processing and reconciliation of transactions, the preparation of regular and credible financial and performance reports, and the review and monitoring of compliance with 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 non-compliance with legislation, or both these aspects.

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 source/destination. The firewall inspects the identification information associated with all communication attempts and compares it to a rule set consistent with the organisation’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 late payments to creditors or statutory obligations as well as payments made for services not utilised or goods not received.

Going concern

The presumption that an auditee will continue to operate in the foreseeable 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 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 the performance of staff and their productivity.

Information technology (IT)

The computer systems used for capturing and reporting financial and non-financial transactions.

IT controls

Computer-related controls ensure the confidentiality, integrity and availability of state information, enable service delivery and promote national security.

IT governance

The leadership, organisational structures and processes which ensure that the auditee's IT resources will sustain its strategies and objectives.

IT infrastructure

The hardware, software, computer-related communications, documentation and skills that are required to support the provision of IT services, together with the environmental infrastructure on which it is built.

IT security management

The controls preventing unauthorised access to auditee networks, operating systems and application systems that generate financial information.

IT service continuity

The processes managing the availability of hardware, system software, application software and data to enable auditees to recover or re-establish information system services in the event of a disaster.

IT user access management

The procedures through which auditees ensure that only valid, authorised users are allowed segregated access to initiate and approve transactions on the information systems.

Internal control / key controls

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.

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.

Irregular expenditure

Expenditure incurred without complying with applicable legislation.

Key drivers of internal control

The three components of internal control that should be addressed to improve audit outcomes, namely leadership, financial and performance management, and governance. (These three components are also defined individually in this glossary.)

Leadership (as one of the drivers of internal control)

The administrative leaders of an auditee, such as heads of departments, chief executive officers and senior management.

It can also refer to the political leadership or the leadership in the province, such as the premier.

Liability

Short-term and long-term debt owed by the auditee.

Material finding (from the audit)

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

Material misstatement
(in the financial statements or annual performance report)

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 the financial statements or annual performance report)

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

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 & coordinating and monitoring departments

National and provincial role players (1) that are directly involved with the management of the auditee (management/leadership assurance) – in other words, the first line of defence; (2) that perform an oversight or governance function, either as an internal governance function or an external monitoring function (internal independent assurance and oversight); and (3) that give an objective assessment of the auditee's reporting (external independent assurance and oversight).

Password

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

Patch management

A piece of programming code that is added to an existing program to repair a deficiency in the functionality of the existing routine or program. It is generally provided in response to an unforeseen need or set of circumstances. Patching is also a common means of adding a new feature or function to a program until the next major version of the software is released.

Platform

A platform consists of an operating system, the computer system's coordinating program, which in turn is built on the instruction set for a processor or microprocessor, and the hardware that performs logical operations and manages data movement in the computer.

Property, infrastructure and equipment
(in financial statements)

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.

Qualified audit opinion (on financial statements)

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.

Receivables / debtors (in financial statements)

Money owed to the auditee by companies, organisations or persons who have procured goods or services from the auditee.

Reconciliation (of accounting records)

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.

Root causes (of audit outcomes being poor or not improving)

The underlying causes or drivers of audit findings; in other words, why the problem occurred. Addressing the root cause helps 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.

Supply chain management

Procuring goods and services through a tender or quotation process and monitoring the quality and timeliness of the goods and services provided.

Vulnerability

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 adverse impact.

Acronyms and abbreviations

AGSA	*Auditor-General of South Africa (the institution)*
Aids	*acquired immunodeficiency syndrome*
APP	*annual performance plan*
APR	*annual performance report*
ART	*anti-retroviral treatment*
ARV	*anti-retroviral*
ASIDI	*accelerated school infrastructure delivery initiative*
BAS	*basic accounting system*
BCP	*business continuity plan*
BI	*business intelligence*
bn (after an amount)	*billion (rand)*
BRRR	*budgetary review and recommendations report*
CAPS	*curriculum assessment policy statement*
CEO	*chief executive officer*
CFO	*chief financial officer*
CGICTPF	*Corporate governance of information and communication technology policy framework*
CIDB	*Construction Industry Development Board*
CIO	*chief information officer*
CIP	*continuous improvement plan*
COGHSTA	*Department of Cooperative Governance, Human Settlements and Traditional Affairs*
CoGTA	*Department of Cooperative Governance and Traditional Affairs*
CRL rights	*Commission for the Promotion and Protection of Cultural, Religious and Linguistic Communities*
CWP	*community work programme*
DBE	*National Department of Basic Education*
DHET	*Department of Higher Education and Training*
DoRA	*Division of Revenue Act*
DPSA	*Department of Public Service and Administration*
DRP	*disaster recovery plan*
EC	*Eastern Cape*
EIG	*education infrastructure grant*

EIS	*education information system*
EPWP	*expanded public works programme*
FMPPI	*Framework for managing programme performance information*
FMPPLA	*Financial Management of Parliament and Legislatures Act*
FS	*Free State*
GP	*Gauteng*
GIS	*geographical information system*
GRAP	*generally recognised accounting practice*
HEDCOM	*Heads of Education Committee*
HIV	*human immunodeficiency virus*
HoD	*head of department*
HR	*human resources*
HSDG	*human settlement development grant*
ICT	*information and communication technology*
IFMS	*integrated financial management system*
IRS	*integrated reporting system*
IT	*information technology*
K (after an amount)	*thousand (rand)*
KZN	*KwaZulu-Natal*
LOGIS	*logistical information system*
LP	*Limpopo*
LTS	*learner transport scheme*
LTSM	*learner teacher support material*
LURTIS	*learner unit record information and tracking system*
m (after an amount)	*million (rand)*
MDB	*Municipal Demarcation Board*
MEC	*member of the executive council of a province*
MIG	*municipal infrastructure grant*
MIS	*management information system*
MP	*Mpumalanga*
MTSF	*Medium term strategic framework 2014-2019*
NAT	*national*

NC	*Northern Cape*
NDP	*National development plan 2030*
NEMA	*National Environmental Management Act, 1998 (Act No. 107 of 1998)*
NEMWA	*National Environmental Management Waste Act, Act No. 59 of 2008*
NHI	*national health insurance*
NHIS	*national health information system*
NW	*North West*
NSDA	*negotiated service delivery agreement*
NSDS III	*National skills development strategy III*
NSNP	*national school nutrition programme*
NSF	*National Skills Fund*
PED	*provincial education department*
Persal	*personnel and salary system*
PFMA	*Public Finance Management Act, 1999 (Act No. 1 of 1999)*
PMTE	*Property Management Trading Entity*
PPPFA	*Preferential Procurement Policy Framework Act*
PRC	*Presidential Review Committee on state-owned entities*
SALGA	*South African Local Government Association*
SAP	*systems, applications and products system*
SASA	*The South African Schools (Act 84 of 1996)*
SA-SAMS	*South African schools administration and management system*
SCM	*supply chain management*
SCoPA	*Standing Committee on Public Accounts*
SETA	*sector education training authority*
SITA	*State Information Technology Agency*
SLAs	*service level agreements*
SSP	*sector skills plan*
TVET	*technical, vocational, education and training*
UAMP	*user assessment management plan*
USDG	*urban settlements development grant*
WC	*Western Cape*