// SECTION 8

Need to know

8.1 OUR AUDIT PROCESS AND FOCUS

WHAT IS OUR AUDIT AND REPORTING PROCESS?

We audit every department and some of the public entities in the country (also called auditees in this report) to report on the quality of their financial statements and performance reports as well as on their compliance with key legislation.

We further assess the root cause of any error or non-compliance, based on the internal control that has failed to prevent or detect it. We report in the following three types of reports:

- We report our findings, the root causes of such findings and our recommendations in **management reports** to the senior management and accounting officers or authorities of auditees, which are also shared with the ministers, members of the executive councils and audit committees.
- Our opinion on the financial statements, material findings on the performance reports and compliance with key legislation, as well as significant deficiencies in internal control, are included in an **audit report**, which is published with the auditee's annual report and dealt with by the public accounts committees and portfolio committees, as applicable.
- Annually, we report on the audit outcomes of all auditees in a **consolidated report** (such as this one), in which we also analyse the root causes that need to be addressed to improve audit outcomes. Before the general report is published, we share the outcomes and root causes with the national and provincial leadership, Parliament and the legislatures, as well as key role players in national and provincial government.

Over the past few years, we have intensified our efforts to assist in improving audit outcomes by identifying the **key controls** that should be in place at auditees, regularly assessing these, and sharing the results of the assessment with ministers, accounting officers and authorities, as well as audit committees.

During the audit process, we work closely with accounting officers or authorities, senior management, audit committees and internal audit units, as they are **key role players** in providing assurance on the credibility of the auditees' financial statements and performance reports as well as on their compliance with legislation.

We also continue to strengthen our relationship with the coordinating and monitoring departments (such as the treasuries, premier's offices and the Department of Planning, Monitoring and Evaluation) as well as Parliament and provincial legislatures, as we are convinced that their involvement and oversight have played – and will continue to play – a crucial role in the performance at departments and public entities. We share our messages on key controls, risk areas and root causes with them, and obtain and monitor their commitments to implementing initiatives that can improve audit outcomes.

The overall audit outcomes fall into five categories:

1. Auditees that receive a **financially unqualified opinion with no findings** are those that are able to:

   - produce financial statements free of material misstatements (material misstatements mean errors or omissions that are so significant that they affect the credibility and reliability of the financial statements)
   - measure and report on their performance in line with the predetermined objectives in their annual performance plan, and in a manner that is useful and reliable
   - comply with key legislation.

   This audit outcome is also commonly referred to as a 'clean audit'.

2. Auditees that receive a **financially unqualified opinion with findings** are those that are able to produce financial statements without material misstatements, but are struggling to:

   - align their performance reports to the predetermined objectives to which they have committed in their annual performance plans
   - set clear performance indicators and targets to measure their performance against their predetermined objectives
   - report reliably on whether they have achieved their performance targets
   - determine which legislation they should comply with, and implement the required policies, procedures and controls to ensure that they comply.

3. Auditees that receive a **financially qualified opinion with findings** face the same challenges as those that are financially unqualified with findings in the areas of reporting on performance and compliance with key legislation. In addition, they are unable to produce credible and reliable financial statements. Their financial statements contain misstatements that they cannot correct before the financial statements are published.

4. The financial statements of auditees that receive an **adverse opinion with findings** include so many material misstatements that we disagree with virtually all the amounts and disclosures in the financial statements.

5. Those auditees with a **disclaimed opinion with findings** cannot provide us with evidence for most of the amounts and disclosures in the financial statements. We are therefore unable to conclude or express an opinion on the credibility of their financial statements. Auditees with adverse and disclaimed opinions are typically also:

- unable to provide sufficient supporting documentation for the achievements they report in their performance reports
- not complying with key legislation.

WHAT IS THE PURPOSE OF THE ANNUAL AUDIT OF THE FINANCIAL STATEMENTS?

The purpose of the annual audit of the **financial statements** is to provide the users thereof with an **opinion** on whether the financial statements fairly present, in all material respects, the key financial information for the reporting period in accordance with the financial reporting framework and applicable legislation. The audit provides the users with reasonable assurance regarding the degree to which the financial statements are reliable and credible on the basis that the audit procedures performed did not reveal any material errors or omissions in the financial statements. We use the term 'material misstatement' to refer to such material errors or omissions.

We report the **poor quality of the financial statements** we receive in the audit reports of some auditees as a material finding on compliance, as it also constitutes non-compliance with the PFMA. The finding is only reported for auditees that are subject to the PFMA and if the financial statements we receive for auditing include material misstatements that could have been prevented or detected if the auditee had an effective internal control system. We do not report a finding if the misstatement resulted from an isolated incident or if it relates to the disclosure of unauthorised, irregular or fruitless and wasteful expenditure identified after the financial statements had been submitted.

WHAT DOES COMPLIANCE WITH KEY LEGISLATION MEAN?

We annually audit and report on **compliance by auditees with key legislation** applicable to financial and performance management and related matters.
We focus on the following areas in our compliance audits, if they apply to the particular auditee: ■ the quality of financial statements submitted for auditing ■ asset and liability management ■ expenditure management ■ unauthorised, irregular, and fruitless and wasteful expenditure ■ consequence management ■ revenue management ■ strategic planning and performance management ■ financial statements and annual report ■ conditional grants ■ procurement and contract management (in other words, SCM).

In our audit reports, we report findings that are material enough to be brought to the attention of auditee management, as well as oversight bodies and the public.

WHAT IS THE SCOPE OF SUPPLY CHAIN MANAGEMENT AUDITS?

We test whether the **prescribed procurement processes** have been followed to ensure that all suppliers are given equal opportunity to compete and that some suppliers are not favoured above others. The principles of a fair, equitable, transparent, competitive and cost-effective SCM process are fundamental to the procurement practices of the public sector, as enshrined in the country's constitution and prescribed in the PFMA and its regulations. The PFMA and these regulations define what processes should be followed to adhere to the constitutional principles, the level of flexibility available, and the documentation requirements.

We also focus on **contract management**, as shortcomings in this area can result in delays, wastage as well as fruitless and wasteful expenditure, which in turn have a direct impact on service delivery.

We further assess the **financial interests of employees of the auditee and their close family members** in suppliers to the auditee. Although there is no legislation that prohibits making awards to suppliers in which state officials have an interest, the **amended Public Service Regulations prohibit employees of departments from doing business with the state** from 1 August 2016. The regulations allowed employees that were doing business with the state on 1 August 2016 time until February 2017 to stop the business or resign as an employee.

WHAT IS IRREGULAR EXPENDITURE?

Irregular expenditure is expenditure that was **not incurred in the manner prescribed by legislation**; in other words, somewhere in the process that led to the expenditure, the auditee did not comply with the applicable legislation.

Such expenditure does **not necessarily mean that money had been wasted or that fraud had been committed**. It is an indicator of non-compliance in the process that needs to be investigated by management to determine whether it was an unintended error, negligence or done with the intention to work against the requirements of legislation (which, for example, require that procurement should be fair, equitable, transparent, competitive and cost-effective).

Through such **investigation**, it is also determined who is responsible and what the impact of the non-compliance is. Based on the investigation, the next steps are determined. One of the steps can be condonement if the non-compliance had no impact and negligence was not proven. Alternatively, if negligence was proven, the steps can be disciplinary steps, the recovery of any losses from the implicated officials or even cancelling a contract or reporting it to the police or an investigating authority.

The PFMA is clear that **accounting officers and authorities are responsible** for preventing irregular expenditure as well as on what process to follow if it has been incurred.

In order to promote transparency and accountability, auditees **should disclose all irregular expenditure identified (whether by the auditee or through the audit process)** in their financial statements with detail on how it had been resolved; in other words, how much had been investigated, recovered or condoned.

WHAT IS FRUITLESS AND WASTEFUL EXPENDITURE?

Fruitless and wasteful expenditure is expenditure that was made in vain and that 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 made for services not used or goods not received.

The PFMA requires accounting officers and accounting authorities to take all **reasonable steps to prevent fruitless and wasteful expenditure**. Auditees should have processes to detect fruitless and wasteful expenditure and disclose the amounts in the financial statements. Fruitless and wasteful expenditure is reported when it is identified – even if the expenditure was incurred in a previous year.

The act also sets out the steps that accounting officers and oversight bodies should take to investigate fruitless and wasteful expenditure to determine whether any officials are liable for the expenditure and to recover the money if liability is proven.

WHAT IS UNAUTHORISED EXPENDITURE?

Unauthorised expenditure refers to expenditure that auditees incurred without provision having been made for it in the approved budget.

The PFMA requires accounting officers to take all **reasonable steps to prevent unauthorised expenditure**. Auditees should have processes to identify any unauthorised expenditure and disclose the amounts in the financial statements. The act also includes the steps that accounting officers and oversight bodies should take to investigate unauthorised expenditure to determine whether any officials are liable for the expenditure and to recover the money if liability is proven.

WHAT ARE CONDITIONAL GRANTS?

Conditional grants are **funds allocated from national government to provincial departments, subject to certain services being delivered or on compliance with specified requirements**.

Conditional grant allocations are approved each year through the Division of Revenue Act. This act indicates the approved allocation per auditee for that particular year, together with a forward estimate for the next two years.

Conditional grants stem from government's vision and priorities as articulated in the MTSF, which focuses on placing the economy on a qualitatively different path that ensures rapid sustainable growth, higher investments, increased employment, reduced inequality and the deracialisation of the economy.

In support of these goals, conditional grants are provided to provincial departments to:

- reduce the concentration of people in urban areas (comprehensive agricultural support programme grant and human settlements development grant)
- increase adequate infrastructure (education infrastructure grant, provincial roads maintenance grant and health facility revitalisation grant)
- improve skills (HIV and Aids grant, EPWP integrated grant for provinces and social sector EPWP incentive grant for provinces).

During our audits, we test compliance with the Division of Revenue Act and the individual grant frameworks, as well as the achievement of planned targets for selected projects or programmes funded by each grant allocation.

WHAT IS THE PURPOSE AND NATURE OF THE ANNUAL AUDIT OF THE PERFORMANCE REPORTS?

Auditees are required to measure their actual service delivery against the performance indicators and targets set for each of their predetermined performance objectives as defined in their annual performance plan, and to report on this in their performance reports.

On an annual basis, we audit **selected material programmes** of departments **and objectives** of public entities to determine whether the information in the performance reports is useful and reliable enough to enable oversight bodies, the public and other users of the reports to assess the performance of the auditee. The programmes and objectives we select are those that are important for delivery by the auditee on its mandate. In the audit report, we report findings that are material enough to be brought to the attention of these users.

As part of the annual audits, we audit the **usefulness of the reported performance information** to determine whether it is presented in the annual report in the prescribed manner and is consistent with the auditee's planned objectives as defined in strategic and annual performance plans. We also assess whether the performance indicators and targets set to measure the achievement of the objectives are:

- well defined (the indicator needs to have a clear, unambiguous definition so that data can be collected consistently, and is easy to understand and use)
- verifiable (it must be possible to validate the processes and systems that produce the indicator)

- specific (so that the nature and the required level of performance can be clearly identified)
- time bound (the time period or deadline for delivery must be specific)
- measurable (so that the required performance can be measured)
- consistent (with the objective, measures and/or targets)
- relevant (so that the required performance can be linked to the achievement of a goal).

WHEN IS HUMAN RESOURCE MANAGEMENT EFFECTIVE?

HR management refers to the **management of an auditee's employees or human resources**. HR management is effective if adequate and sufficiently skilled staff members are in place and if their performance and productivity are properly managed.

Our audits include an assessment of HR management, focusing on the following areas: ▪ HR planning and organisation ▪ management of vacancies ▪ appointment processes ▪ performance management ▪ acting positions ▪ management of leave and overtime.

Our audits further look at the management of vacancies and stability in key positions, the competencies of key officials, performance management as well as consequences for transgressions, as these matters directly influence the quality of auditees' financial and performance reports and their compliance with legislation.

Based on the results of these audits, we assess the status of auditees' HR management controls.

WHEN ARE INTERNAL CONTROLS EFFECTIVE AND EFFICIENT?

A key responsibility of accounting officers, senior managers and officials is to **implement and maintain effective and efficient systems of internal control**.

We assess the internal controls to determine the effectiveness of their design and implementation in ensuring reliable financial and performance reporting and compliance with legislation. This consists of all the policies and procedures implemented by 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. To make it easier to implement corrective action, we categorise the principles of the different components of internal control under leadership, financial and performance management, or governance. We call these the drivers of internal control.

The key basic controls that auditees should focus on are outlined.

Providing effective leadership

In order to improve and sustain audit outcomes, auditees require **effective leadership** that is based on a culture of honesty, ethical business practices and good governance to protect and enhance the interests of the auditee.

Audit action plans to address internal control deficiencies

Developing and monitoring the implementation of action plans to address identified internal control deficiencies are key elements of internal control, which are the responsibility of heads of departments, chief executive officers and their senior management team.

Some of the matters requiring attention include the following:

- Setting action plans to specifically address the external and internal audit findings.
- Assigning clear responsibility to specific staff to carry out action plans.
- Monitoring audit action plans to ensure that the responsibilities assigned are carried out effectively and consistently.
- Developing audit action plans early enough in the financial year to resolve matters by year-end.

Proper record keeping and document control

Proper and timely record keeping ensures that **complete, relevant and accurate information** is accessible and available to support financial and performance reporting. Sound record keeping will also enable senior management to hold staff accountable for their actions. A lack of documentation affects all areas of the audit outcomes.

Some of the matters requiring attention include the following:

- Establishing proper record keeping so that records supporting financial and performance information as well as compliance with key legislation can be made available when required for audit purposes.
- Implementing policies, procedures and monitoring mechanisms to manage records, and making staff members aware of their responsibilities in this regard.

Implementing controls over daily and monthly processing and reconciling of transactions

Controls should be in place to ensure that **transactions are processed accurately, completely and timeously**, which in turn will reduce errors and omissions in financial and performance reports.

Some of the matters requiring attention include the following:

- Daily capturing of financial transactions, supervisory reviews of captured information, and independent monthly reconciliations of key accounts.
- Collecting performance information at intervals appropriate for monitoring, setting service delivery targets and milestones, and validating recorded information.
- Confirming that legislative requirements and policies have been complied with before initiating transactions.

Reviewing and monitoring compliance with legislation

Auditees need to have mechanisms that can **identify applicable legislation as well as changes to legislation**, assess the requirements of legislation, and implement processes to ensure and monitor compliance with legislation.

WHAT IS INFORMATION TECHNOLOGY AND WHAT ARE INFORMATION TECHNOLOGY CONTROLS?

IT refers to the computer systems used for recording, processing and reporting financial and non-financial transactions. IT controls ensure the confidentiality, integrity and availability of state information, enable service delivery, and promote national security. Good IT governance, effective IT management and a secure IT infrastructure are therefore essential.

Non-complex and complex information technology environments

As per our new audit methodology, we differentiate between **non-complex** and **complex** IT environments, as follows:

Non-complex environment – level 1 (low risk)

This is the lower end of the spectrum for IT sophistication and relevance. The auditee uses one server associated with financial reporting and/or performance information, a limited number of workstations, no remote locations, commercial off-the-shelf applications and infrastructure, vendors to perform updates and maintenance on the system, little emerging or advanced technology, and a few or no online and e-commerce transactions.

Key controls over financial reporting and/or performance information are not overly reliant on IT, are embedded in the commercial off-the-shelf applications, or are limited to very few manual processes and controls. Many small to medium-sized entities fall into this category.

Complex environment – levels 2 and 3 (medium and high risk)

This is the middle to high end of the spectrum. These auditees have the following characteristics:

- Use more than one server associated with financial reporting and/or performance information.
- Have remote locations.
- Employ one or more network operating system or non-standard ones.
- Have more workstations in total.
- Use some customisation of application software or have a relatively complex configuration of commercial off-the-shelf applications.
- Use enterprise resource planning systems and/or write their own custom software.
- Perform updates and maintenance on the system centrally onsite or through vendors, or perform centralised updates and maintenance on the system and distribute these to decentralised sites or through onsite vendors.
- Employ a few to moderate or a large number of emerging or advanced technologies.
- Enter into either a few or a large number of online and e-commerce transactions.
- Rely heavily on IT key controls over financial and/or performance information.

An auditee running transversal systems would also fall into this category. Information systems for which certain IT processes are managed centrally, but which are used by various auditees who have limited responsibility regarding the design and enhancement of the system, will also be classified as high risk at a national level.

Which information technology controls do we audit?

During our audits, we assess the IT controls that focus on IT governance, security management, user access management and IT service continuity – as discussed further down. To evaluate the status of the IT controls in the areas we audit, we group them into the following three categories, with reference to the control measures that should be in place:

1. **Where IT controls are being designed**, management should ensure that the controls would reduce risks and threats to IT systems.
2. **Where IT controls are being implemented**, management should ensure that the designed controls are implemented and embedded in IT processes and systems. Particular attention should be paid to ensuring

that staff members are aware of and understand the IT controls being implemented, as well as their roles and responsibilities in this regard.

3. **Where IT controls have been embedded and are functioning effectively**, management should ensure that the IT controls that have been designed and implemented are functioning effectively at all times. Management should sustain these IT controls through disciplined and consistent daily, monthly and quarterly IT operational practices.

Information technology governance

This refers to the leadership, organisational structures and processes which ensure that the auditee's IT resources will sustain its business strategies and objectives. Effective IT governance is essential for the overall well-being of an auditee's IT function and ensures that the auditee's IT control environment functions well and enables service delivery.

Security management

This refers to the controls preventing unauthorised access to the computer networks, computer operating systems and application systems that generate and prepare financial and performance information.

User access management

These are measures designed by business management to prevent and detect the risk of unauthorised access to, and the creation or amendment of, financial and performance information stored in the application systems.

Information technology service continuity

These controls enable auditees to recover within a reasonable time the critical business operations and application systems that would be affected by disasters or major system disruptions.

WHAT ARE ROOT CAUSES?

Root causes are the **underlying causes or drivers of audit findings**; in other words, the reason why the problem occurred. Addressing the root cause helps to ensure that the actions address the real issue, thus preventing or reducing incidents of recurrence, rather than simply providing a one-time or short-term solution.

Our audits include an **assessment of the root causes of audit findings**, based on the identification of internal controls that have failed to prevent or detect the error in the financial statements and performance reports or that have led to non-compliance with legislation. These root causes are confirmed with management and shared in the management report with the accounting officer and the executive authorities. We also include the root causes of material findings reported as internal control deficiencies in the audit report, classified under the key drivers of leadership, financial and performance management, or governance.

WHO PROVIDES ASSURANCE?

Ministers, members of the executive councils and accounting officers use the **annual report** to report on the financial position of auditees, their performance against predetermined objectives, and overall governance; while one of the important **oversight functions of legislatures is to consider auditees' annual reports**. To perform their oversight function, they need assurance that the information in the annual report is credible. To this end, the annual report also includes our audit report, which provides assurance on the credibility of the financial statements, the performance report and the auditee's compliance with legislation.

Our reporting and the oversight processes reflect on history, as they take place after the financial year. Many other role players contribute throughout the year to the credibility of financial and performance information and compliance with legislation by ensuring that adequate internal controls are implemented.

The mandates of these role players differ from ours, and we have categorised them as follows:

- Those directly involved in the management of the auditee (management or leadership assurance).
- Those that perform an oversight or governance function, either as an internal governance function or as an external monitoring function (internal independent assurance and oversight).
- The independent assurance providers that give an objective assessment of the auditee's reporting (external independent assurance and oversight).

We **assess the level of assurance** provided by the role players based on the **status of auditees' internal controls and the impact of the different role players on these controls**. In the current environment, which is characterised by inadequate internal controls, corrected and uncorrected material misstatements in financial and performance information, and widespread non-compliance with legislation, all role players need to provide an extensive level of assurance.

WHAT IS THE ROLE OF EACH KEY ROLE PLAYER IN PROVIDING ASSURANCE?

Senior management

Senior management, which includes the chief financial officer, chief information officer and head of the SCM unit, provides assurance by implementing the following basic financial and performance controls:

- Ensure proper record keeping so that complete, relevant and accurate information is accessible and available to support financial and performance reporting.
- Implement controls over daily and monthly processing and reconciling of transactions.

- Prepare regular, accurate and complete financial and performance reports that are supported and evidenced by reliable information.

- Review and monitor compliance with applicable legislation.

- Design and implement formal controls over IT systems.

Accounting officers or accounting authorities

While we recognise that accounting officers and authorities depend on senior management for designing and implementing the required financial and performance management controls, they are responsible for creating an environment that helps to improve such controls.

The responsibilities of accounting officers and authorities are clearly described in section 38 (for departments) and section 51 (for public entities) of the PFMA. This includes their responsibility to ensure that:

- there are consequences for transgressions through disciplinary steps against officials who contravene the PFMA and make or permit unauthorised, irregular, and fruitless and wasteful expenditure

- appropriate, efficient and effective systems or policies are implemented and maintained for, among other, internal control, internal audit and SCM

- resources are used effectively, efficiently, economically and transparently

- effective and appropriate steps are taken to collect all money due to the auditee

- assets and liabilities are properly managed, including the safeguarding thereof

- expenditure is in accordance with the budget (including steps to prevent overspending).

Executive authorities

The executive authorities (ministers and members of the executive councils) have specific monitoring and oversight responsibilities in their portfolios in terms of the PFMA and the Public Service Act. They are well placed to bring about improvements in the audit outcomes by becoming more actively involved in key governance matters and by managing the performance of the accounting officers and authorities.

We are convinced that the oversight and monitoring roles of the executive strengthen the assurance processes significantly, and this has had a positive impact on the audit outcomes in the past year. We therefore undertake to carry on with our engagements with them, but with greater emphasis on quality conversations that will yield a stronger impact.

Internal audit units

The internal audit units assist accounting officers and authorities in the execution of their duties by providing independent assurance on internal controls, financial information, risk management, performance management and compliance with legislation. The establishment of internal audit units is a requirement of legislation.

Audit committees

An audit committee is an independent body, created in terms of legislation, which advises the accounting officer or authority, senior management and executive authorities on matters such as internal controls, risk management, performance management and compliance with legislation. The committee is further required to provide assurance on the adequacy, reliability and accuracy of financial and performance information.

Coordinating or monitoring departments

At national and provincial level, some departments play a coordinating and monitoring role as defined in legislation and in their mandates, which should contribute to the overall assurance process. These departments are the National Treasury, provincial treasuries, offices of the premier, and Department of Planning, Monitoring and Evaluation. We assess the impact of these departments on the controls of the auditees based on our interactions with them, commitments given and honoured as well as the impact of their actions and initiatives.

Public accounts committees and portfolio committees

Parliament and the provincial legislatures have a constitutional mandate to oversee executive action and ensure compliance with legislation. These institutions conduct oversight through committees established in line with the rules of Parliament and the provincial legislatures. Portfolio committees are required to assess the strategic and annual performance plans of departments and public entities to effectively fulfil their oversight role.

Informed by our constitutional mandate, we enable oversight, accountability and governance in the public sector through our regular engagements with Parliament and the provincial legislatures. We do this through oversight leadership and portfolio committee engagements, during which we present and discuss key controls and compliance findings arising from the audit process and the related root causes. The discussions include our recommendations on focus areas that require oversight intervention. We hope that through these interactions, specific oversight efforts will lead to improved governance and accountability in the public sector.

8.2 GLOSSARY OF KEY TERMINOLOGY USED IN THIS REPORT

Asset (in financial statements)	Any item belonging to the auditee, including property, infrastructure, equipment, cash, and debt due to the auditee.
Backup (IT)	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.
Business continuity plan (IT)	A business continuity plan is a plan to continue operations if an auditee 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 auditee 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 auditee or data centre operations would relocate to a recovery site.
Cash flow (in financial statements)	The flow of money from operations: incoming funds are revenue (cash inflow) and outgoing funds are expenses (cash outflow).
Chief information officer or government information technology officer	The most senior official of the auditee who is accountable for aligning IT and business strategies; for planning, resourcing and managing the delivery of IT services and information; and for the deployment of the associated human resources. The chief information officers in the South African public sector are referred to as government IT officers. The position was established by a cabinet memorandum in 2000.
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.
Configuration (IT)	The complete technical description required to build, test, accept, install, operate, maintain and support a system.
Creditors	Persons, companies or organisations to whom the auditee owes money 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 within 12 months. All other assets are classified as non-current, and typically include property, plant and equipment as well as long-term investments.
Current liability (in financial statements)	Money owed by the auditee to companies, organisations or persons who have supplied goods and services to the auditee.
Disaster recovery plan (IT)	A documented process or set of procedures to recover and protect an auditee's IT infrastructure in the event of a disaster. Usually documented in written form, the plan specifies the procedures that an auditee 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).
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 processing and reconciling transactions, the preparation of regular and credible financial and performance reports as well as the review and monitoring of compliance with key legislation.

Firewall (IT)	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 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.
Governance (as one of the drivers of internal control)	The governance structures (audit committees) and processes (internal audit and risk management) of an auditee.
Implementing agent	Government institutions (e.g. the Independent Development Trust), non-governmental organisations or private sector entities appointed by the auditee to manage, implement and deliver on projects.
IT infrastructure (IT)	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.
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).
Material finding (from the audit)	An audit finding on the quality of the 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 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 performance reports)	Incorrect or omitted information in the financial statements or performance report.
Patch management (IT)	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 (IT)	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.
Public Audit Act (Act No. 25 of 2004)	This is the Auditor-General of South Africa's enabling legislation. The objective of the act is to give effect to the provisions of our country's constitution by establishing and assigning functions to an auditor-general and by providing for the auditing of institutions in the public sector.
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.
Receivables or debtors (in financial statements)	Money owed to the auditee by companies, organisations or persons who have procured goods and services from the auditee.

Status of records review	A process whereby the auditor performs basic review procedures to identify risks and areas of concern for discussion with the accounting officer. The purpose of the status of records review is to: • ensure that there is a system of early warning to the accounting officer on challenges that may compromise good financial and performance management and compliance with legislation • demonstrate to the accounting officer a deepened level of understanding of the business of the auditee and the value added by the auditor • contribute to capacitating the accounting officer and senior management in instilling good practices of regular reporting, review and oversight • identify risks early and throughout the audit cycle to respond to these timeously and correctly.
Virement	The utilisation (transfer) of a saving from one programme towards the defrayment of excess expenditure under another programme within the same vote (department).
Vulnerability (IT)	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.
Vulnerable financial position (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.