SECTION 6: GOVERNANCE AND CONTROLS

Figure 1: Overall drivers of internal control did not improve

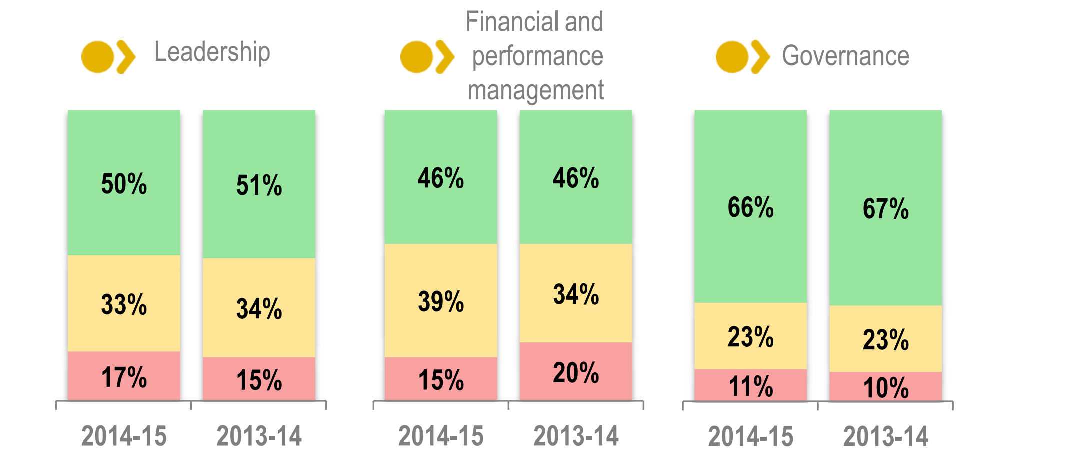


Figure 2: Aspect of drivers of internal control requiring most attention

Audit areas and number of auditees

	Financial statements			Performance reports			Compliance with legislation		
Effective leadership	70%	23%	7%	73%	20%	7%	65%	26%	9%
Human resource controls	50%	35%	15%	59%	29%	12%	49%	34%	16%
Audit action plans	49%	37%	14%	56%	31%	13%	50%	35%	15%
IT governance and controls	28%	53%	19%	Not assessed			Not assessed		
Proper record keeping	49%	34%	17%	54%	29%	17%	54%	32%	14%
Daily and monthly controls	44%	40%	16%	58%	26%	16%	56%	33%	11%
Review and monitor compliance	40%	42%	18%	55%	28%	17%	29%	46%	25%

Table 1: Progress made in improving drivers of internal control

Portfolio	Leadership	Financial and performance management	Governance
National auditees	►	►	►
Eastern Cape	▼	►	▲
Free State	▲	▲	▲
Gauteng	►	►	►
KwaZulu-Natal	▲	►	▼
Limpopo	▲	▲	▲
Mpumalanga	▼	▼	►
Northern Cape	▼	►	►
North West	►	►	▲
Western Cape	►	►	►

🟩 Good 🟨 Concerning 🟥 Intervention required (Also applies to the remainder of this section)

6.1 Status of internal controls

A key responsibility of accounting officers, senior managers and officials is to implement and maintain effective and efficient systems of internal control. We assessed the internal controls to determine the effectiveness of their design and implementation in ensuring reliable financial and performance reporting and compliance with legislation. To make it easier to implement corrective action, we categorised the principles of the different components of internal control as either leadership, financial and performance management, or governance. We call these the drivers of internal control.

Status of the drivers of internal controls

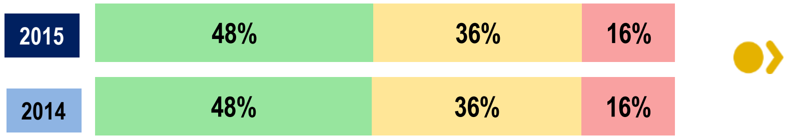
Figure 1 shows the status of the different areas of internal control and the overall movement since the previous year. The lack of overall improvement is the result of some national and provincial auditees having made progress, which was offset by the regression and stagnation of other auditees as seen in table one. Overall departments have shown an improvement, but public entities regressed slightly.

In sections 3.1 (quality of financial statements), 4 (quality of APRs) and 3.2 (compliance with legislation) we commented broadly on those key controls that should receive attention to improve or sustain the audit outcomes.

Figure 2 shows the status of the specific control areas requiring the most attention. The remainder of this section provides more detail on the basic controls and disciplines that need to be strengthened to improve the quality of the financial and performance reports and prevent non-compliance with legislation.

Sections 5.1 and 6.2 provide further information on the status of the human resource controls and the ICT governance and controls. The root causes have a significant impact on the effectiveness of internal controls. Section 6.3 describes the most common root causes that should be addressed if the systems of internal control are to be significantly improved.

Providing effective leadership



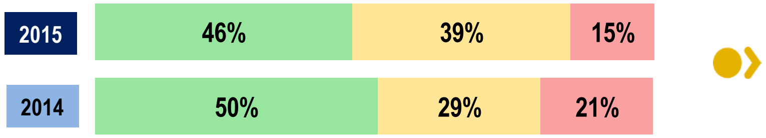
To improve and sustain audit outcomes, auditees require effective leadership that is based on a culture of honesty, ethical business practices and good governance, protecting and enhancing the interests of the entity.

Leadership controls still requiring attention at approximately a third of auditees include the following key aspects:

- Implementing formal codes of conduct and communicating their existence and continued applicability to officials periodically.
- Monitoring the performance of key officials in maintaining adequate systems of internal control that ensure credible monthly financial reporting, reliable reporting against predetermined objectives and compliance with legislation.
- Establishing clear lines of accountability.
- Taking corrective/disciplinary action against key officials for misconduct.
- Honouring commitments made for interventions following the 2013-14 audit outcomes.

Effective leadership controls did not improve at departments (61%) or public entities (72%).

Audit action plans to address internal control deficiencies



Developing action plans and monitoring their implementation to address identified internal control deficiencies is a key element of internal control that is the responsibility of heads of departments, chief executive officers and their senior management team.

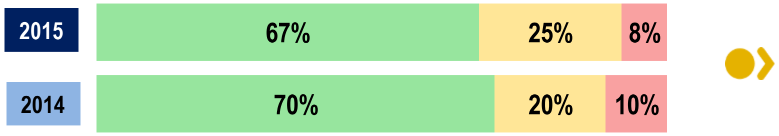
Internal controls in the form of audit action plans assessed as being 'good' improved at departments to 37%, but remained unchanged for public entities at 54%.

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 to ensure that the responsibilities assigned were carried out effectively and consistently.
- Developing audit action plans early enough in the financial year to resolve matters by year-end.

- Ensuring that audit action plans address all three areas of audit outcomes: qualifications, findings on APRs and compliance with legislation.
- Focusing the actions to be taken on the root causes of the findings, thereby ensuring sustainable solutions are found.

Proper record keeping and document control



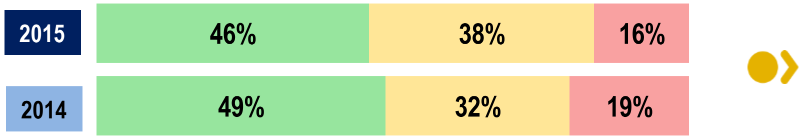
Proper record keeping in a timely manner ensures that complete, relevant and accurate information is accessible and available to support financial and performance reporting. Sound record keeping will also enable senior management to hold staff accountable for their actions.

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 legislation, and can be made available when required for auditing purposes.
- Having policies, procedures and monitoring mechanisms to manage records, and making staff aware of their responsibilities in this regard.

Record keeping and document controls assessed as being ‘good’ remained unchanged at 39% at departments while regressing at public entities to 50%, resulting in no significant overall improvement.

Implement controls over daily and monthly processing and reconciling of transactions



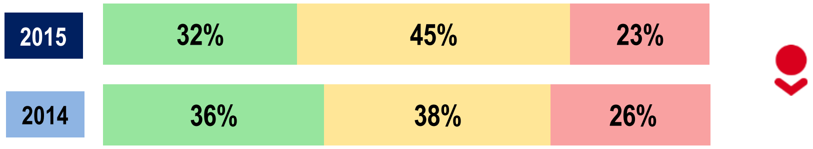
Controls should ensure that transactions are processed in an accurate, complete and timely manner, which will reduce the errors and omissions in financial and performance reports.

Some of the matters requiring attention include the following:

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

Good processing controls were established at 41% of departments (unchanged); while regressing at public entities from 55% to 50%.

Review and monitor compliance with legislation



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

As detailed in section 3.2, many auditees did not comply with legislation. This indicates that the internal controls of most auditees not only failed to prevent non-compliance with legislation, but also failed to detect the deviations in time. Some deviations were only detected and responded to following our audits.

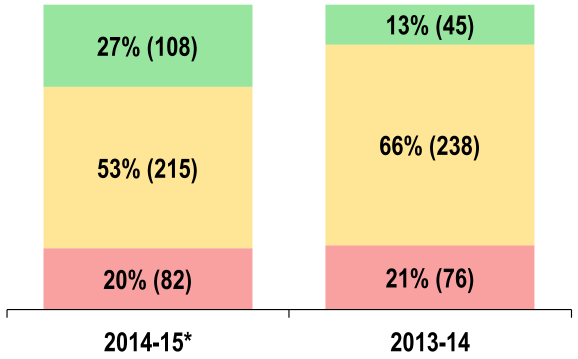
At 28% of departments and 50% of public entities, controls to prevent or detect non-compliance with legislation were clearly short of the required level. Further, these controls improved over the previous year only at public entities.

Compliance monitoring matters requiring attention are included in our recommendations in section 3.2.

Annexure 3 details the status of auditees’ key controls and the movement since the previous year.

[This page is intentionaly left blank]

Figure 1: Status of information technology



* *IT governance has now been incorporated in the overall assessment, thus contributing to the improvement*

Figure 2: Status on the information technology focus areas

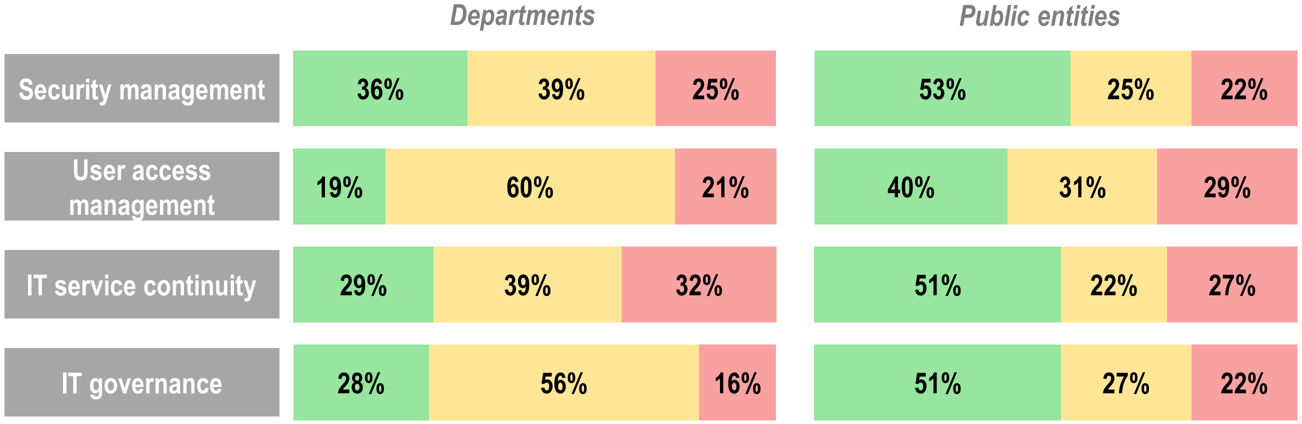
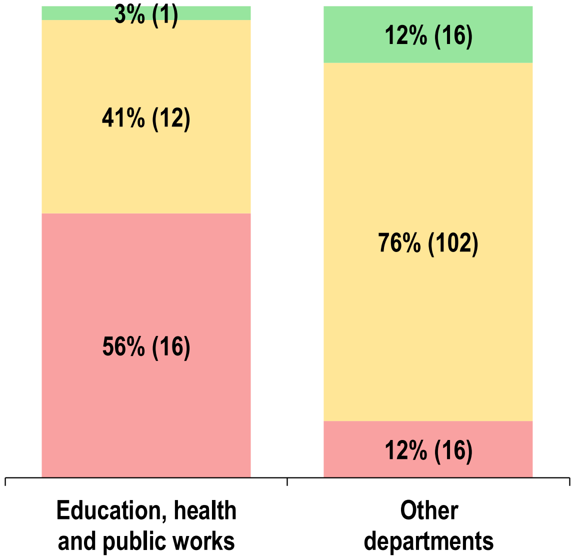


Figure 3: Progress made in improving findings

	Security management	*User access management*	*IT service continuity*	*IT governance*
National	🟢↑	🟡→	🟢↑	🟢↑
Eastern Cape	🟡→	🟡→	🟡→	🟢↑
Free State	🔴↓	🟢↑	🟢↑	🟢↑
Gauteng	🟡→	🔴↓	🔴↓	🟢↑
KwaZulu-Natal	🟢↑	🟢↑	🟢↑	🟢↑
Limpopo	🟢↑	🟢↑	🟡→	🟢↑
Mpumalanga	🟢↑	🟢↑	🟢↑	🟢↑
Northern Cape	🔴↓	🟢↑	🟢↑	🟢↑
North West	🟢↑	🟢↑	🟢↑	🟢↑
Western Cape	🔴↓	🔴↓	🟢↑	🟢↑
Public entities	🟢↑	🟢↑	🟡→	🟢↑

Figure 4: Status of information technology – Education, health and public works vs. other departments



🟩 Good 🟨 Concerning 🟥 Intervention required

6.2 Information technology controls

IT controls ensure the confidentiality, integrity and availability of state information, enables service delivery and promotes national security. It is thus essential for good IT governance, effective IT management and a secure IT infrastructure to be in place.

Effective IT governance underpins the overall well-being of an organisation's IT function and ensures that the organisation's IT control environment functions well and enables service delivery.

6.2.1 Overview of the status of information technology focus areas

Our audit included an assessment of the IT controls in the areas of IT governance, security management, user access management and IT service continuity. Figure 1 shows that there has been a reduction since the previous year in the number of auditees that had audit findings on IT controls and that IT governance has been incorporated into the overall assessment. An analysis of the audit outcomes indicated that at a small number of auditees good progress has been made in addressing previously raised findings.

Figure 2 above outlines the status of the controls per focus area audited at departments and public entities and indicates whether the IT controls are good, concerning, or require intervention. Figure 3 indicates the progress made since the previous year in addressing areas of concern at departments at both national and provincial levels, as well as at public entities.

The most common findings were the following:

- IT governance frameworks and structures had not been adequately designed and implemented for the majority of the departments' IT environments, while public entities were more successful in the design, implementation and operating effectiveness of IT governance.
- Most of the departments and some public entities still experienced challenges that emanated from a lack of adequately designed security policies and procedures, while some auditees who had already designed adequate security policies and procedures had not succeeded in implementing them successfully.
- The design of user access management policies and procedures remained a challenge at most of the departments and public entities, while departments and public entities where user access management policies and procedures had been developed experienced difficulties in implementing them. However, good progress had been made at a small number of auditees in the implementation of user access management policies and procedures.
- Most of the departments and some public entities still experienced challenges with the design and implementation of appropriate business continuity plans (BCPs) and disaster recovery plans (DRPs). The management of backups also remained a challenge as most of the auditees did not test their backups to ensure that they could be restored when required. In the case of departments that make use of transversal systems, the data hosted on these systems is available at the disaster recovery site of the State Information Technology Agency (SITA). In all other cases, both departments and entities have to make provision for their own data recovery strategies.

Impact of transversal IT systems on audit outcomes

Departments use transversal systems, such as the basic accounting system (BAS), personnel salary system (Persal) and logistical information system (Logis), to manage financial information. Transversal systems are centrally hosted, managed and maintained by government.

The audit outcomes reported for departments related to weaknesses in manual controls that gave rise to material misstatements and were therefore not the result of weaknesses in the IT controls of transversal systems. Manual controls are internal controls implemented by management to ensure the accurate, timely and complete initiation, recording, processing and correction of transactions.

Integrated financial management system project currently in process

Various challenges have been identified in the processes followed for the integrated financial management system (IFMS) project, which led to the delays and challenges outlined below.

The IFMS project was initiated in 2002 to replace the ageing transversal financial systems, namely BAS, Persal and Logis. Cabinet approved the project, which was intended to commence in 2005 with an estimated project timeline of seven years. However, despite project spend amounting to approximately R1,1 billion as at 31 March 2015 it has not yet been implemented. A new technological approach to the IFMS was approved by cabinet on 20 November 2013 and the incomplete modules were therefore placed on hold. Subsequent to the approval of the new approach the National Treasury revised its business case and requirements in line with the new direction for the IFMS solution. The National Treasury also prioritised the embedding and formalising of project governance processes during the current and next financial year and aims to implement the revised IFMS solution by 2022.

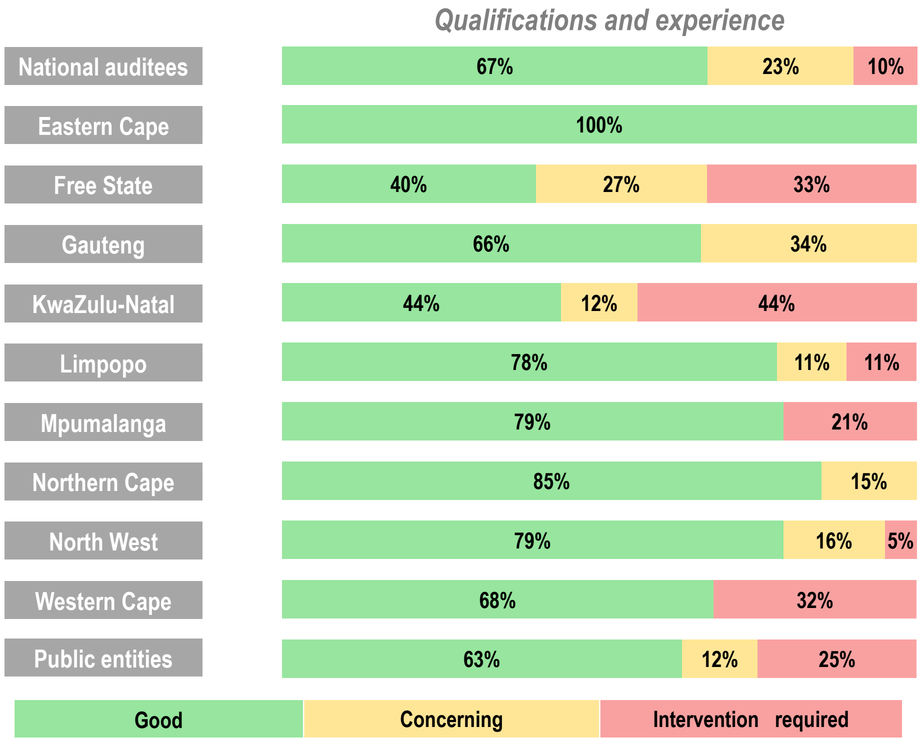
Evaluation of qualifications and experience of chief information officers

Figure 5 indicates that, for the most part, the qualifications and experience of the chief information officers/ IT managers in government are good.

Most of the chief information officers/ IT managers at departments and public entities had the qualifications and experience required to implement the IT governance structures and controls that would ensure improvement in the IT controls of government.

However, smaller public entities did not have the funding and capacity required to assign IT roles and responsibilities to a dedicated individual with the necessary skill and the required qualifications. Furthermore, in some provinces IT departments were operating at the level of deputy director or assistant director, which had a negative effect on the design and implementation of the policies and procedures required for a strong control environment to support business objectives.

Figure 5: Qualifications and experience – chief information officers/ IT managers



e-Government, e-health and e-education strategies

e-Government:

The minister of Public Service and Administration, the Government Information Technology Officer's Council (GITOC), the minister of Telecommunications and Postal Service and the State Information Technology Agency (SITA) are expected to participate in the implementation of e-government.
The e-government strategy is intended to provide a more coordinated and citizen-driven focus to the country's e-government initiatives, thus ensuring that government brings services closer to citizens through an organised and holistic adoption of ICT. The strategy is necessary to provide a clear road map for the processes and initiatives that need to be undertaken for the successful implementation of e-government. This will ensure the effective and efficient use of existing resources, coordinated efforts and sharing of common resources for the e-government services.

The office of the government chief information officer at the DPSA experienced challenges with regard to the stability of the leadership within the branch as the position of the government chief information officer was filled by an officer appointed on a short-term contract that has been renewed on a continuous basis over the past three years.

The majority of government IT officers did not understand the strategic business issues of their departments, which posed a key limitation on their ability to contribute to the initiatives driven by their departments. Some of the government IT officers were not involved in the strategic IT-driven initiatives undertaken by their departments.

e-Health:

The e-Health Strategy South Africa 2012-16 for the public health sector provides the road map for achieving a well-functioning National Health Information System (NHIS). The strategic priorities and target dates have been defined and include various projects to be executed over the duration of the strategy.
An evaluation of the progress to date has to take into consideration that the implementation of the strategy was delayed due to the national department's change to a repeatable process management methodology. As a result, the strategic priorities were redefined and key priorities aimed at enabling e-health were incorporated into the 700 public health care facilities piloted in the National Health Insurance (NHI) project. This project is aimed at reducing waiting times, improving data quality and integrity, as well as timely access to data, streamlining registers and strengthening information management.

The systems used by hospitals to order medication from depots were not integrated to ensure that adequate stock levels would be maintained, while decentralised networks hampered connectivity between hospitals, provincial departments and depots, and system downtime due to slow connectivity issues created problems in the provinces.

e-Education:

The *White paper on e-education* (2004) revolves around the use of ICT to accelerate the achievement of national education goals. The main intended outcome is to increase access to ICT to support curriculum delivery and improve learner attainment. This outcome has, however, been delayed by key challenges such as the following:

- ICT infrastructure provisioning to schools is largely dependent on the capacity of the nine provincial education departments and these departments have to contend with budget and staff constraints. Provinces also have various other priorities that are often regarded as more important than ICT initiatives.
- Broadband connectivity is a challenge, especially in rural areas.
- Many teachers are experiencing difficulties in using ICT.

The Department of Basic Education has put measures in place to accelerate the achievement of e-education in South African schools, which include deliverables and activities such as electronic content resource development and distribution; professional ICT development for management, teaching and learning; access to ICT infrastructure and connectivity. Furthermore, ICT resource centres are also being established in the provinces with the assistance of the private sector.

Status of controls at the departments of education, health and public works vs. that of other departments

Figure 4 indicates the status of the IT controls in the areas we audited at the departments of education, health and public works vs. that of other departments. It shows the number of auditees where the IT controls are good, concerning, or require intervention.

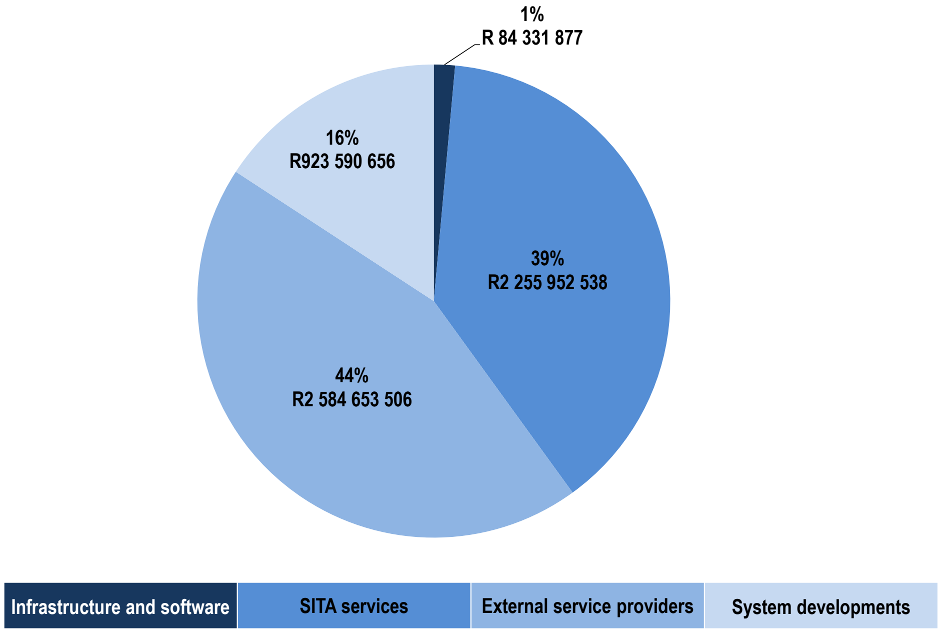
At 56% of the departments of education, health and public works at both provincial and national level intervention is required, compared to only 12% of other departments. Most of the findings raised in previous years at these three departments have not been addressed. The health and education sectors, in particular, experienced challenges with the design and implementation of IT controls, but in some provinces the departments of public works have shown some improvement since the previous year.

Expenses related to information technology at the provincial and national departments

Figure 6 provides a breakdown of the approximate IT-related expenditure in terms of infrastructure and software, SITA services, external service providers and project developments.

The split between the amounts spent on SITA support services and services rendered by external service providers was more or less equal and overall represented 83% of the total amount spent. Although the amount spent on procuring services represented the largest part of the IT expenditure, the performance monitoring processes for services provided by service providers were found to be inadequate, which resulted in payments being made by departments without monitoring whether services were delivered at the agreed upon level of quality. System developments to enhance systems only represented 16% of the expenses, while only 1% was spent on infrastructure and software licensing.

Figure 6: Expenses related to information technology at national and provincial departments



Most common root causes and the actions taken to address them

- The framework for corporate governance of ICT developed by the DPSA was adopted by most departments without customising it for their own departmental environments.
- Although the skills and experience at departments and public entities were adequate at chief information officer/ IT manager level, they were not successful in attracting staff to fill vacant key positions, such as system

controllers and information security officers. Some of these IT divisions were, furthermore, not operating on a strategic level to influence the design and implementation of adequate policies and procedures.

- Staff were not fulfilling their responsibilities by ensuring compliance with the controls established to secure and regulate their departments' IT environments.
- The approval of IT policies and procedures was not prioritised.
- The performance monitoring processes of IT service providers were not adequately enforced to ensure that services were rendered at the agreed upon level of quality or standard.

6.2.2 Recommendations

The following actions should be taken to address the findings and root causes:

- IT governance frameworks and structures should be customised by auditees for their specific environments to ensure that IT controls are governed appropriately. Continuous monitoring of the implementation and operating effectiveness of governance structures already established should be prioritised.
- Management should enforce consequence management where repeat IT findings are not addressed.
- Internal audit units and audit committees should play a more active and effective role in tracking the progress made in implementing management commitments in respect of previously raised IT audit findings and in improving IT controls generally.
- Management should ensure that service providers are monitored on a regular basis and that corrective actions are taken against them where deviations from the expected quality and standards are detected.

6.3 Summary of root causes

To assist auditee management and those charged with governance and oversight, our audits continue to include an assessment of the root causes of audit findings, based on us having identified the internal controls that failed to prevent or detect the error in financial statements and APRs as well as non-compliance with legislation.

These root causes were confirmed with management and shared in the management report with the accounting officer and the executive authorities. We also included the root causes of material findings reported in the audit report as internal control deficiencies in the audit report, classified under the key drivers of leadership, financial and performance management, or governance (refer section 6.1).

Figure 1: Status of overall root causes

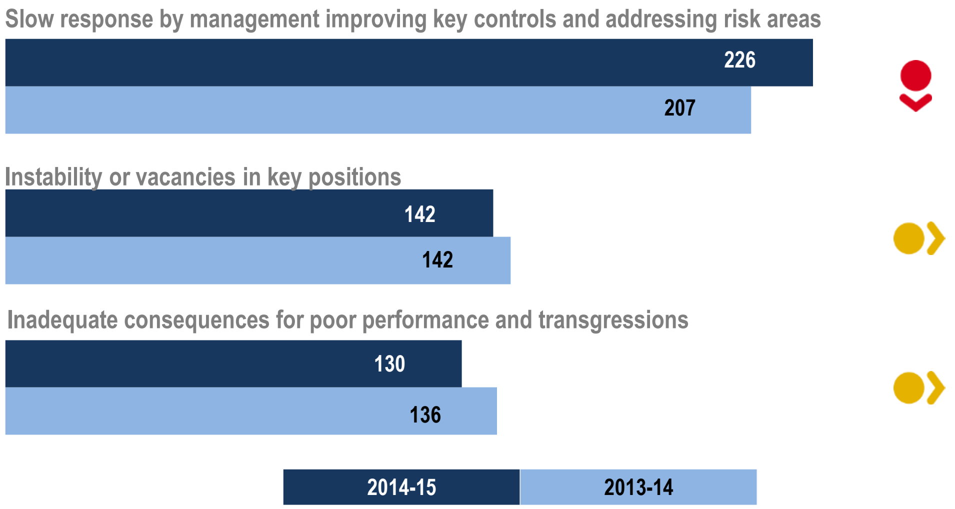


Figure 1 shows the most common root causes we identified which affect the rate at which audit outcomes improve.

Figure 2: Analysis of top three root causes in the three audit areas

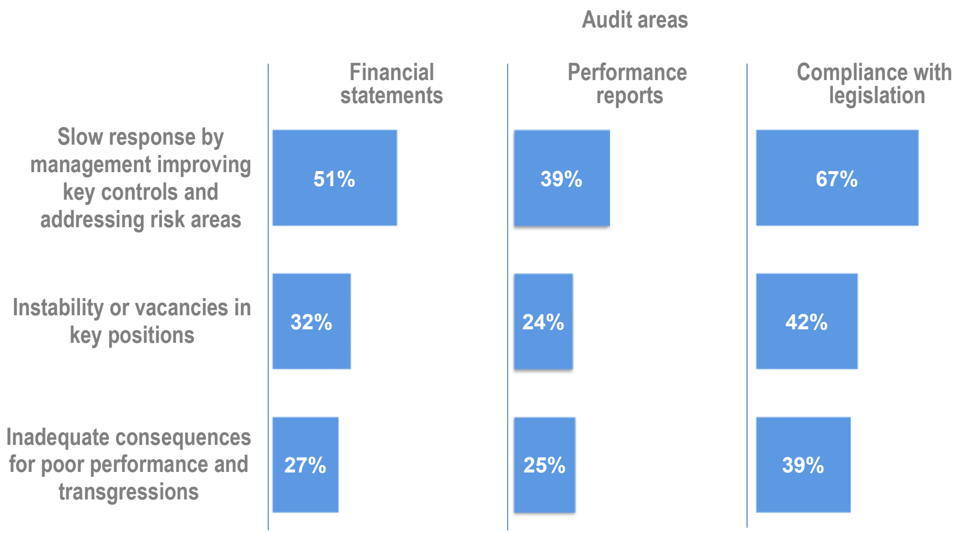


Figure 2 shows the percentage of auditees affected by the top three root causes in the three areas that we audit and report on.

The quality of financial statements is significantly affected by the slow response by management in improving internal controls (51%). The quality of performance reports are almost equally affected by each of the three root causes. Individually and jointly slow response by management (67%), instability or vacancies in key positions (42%) as well as inadequate consequences (39%) are at the root of non-compliance with legislation.

We next summarise the three most common root causes of audit outcomes and we provide recommendations to address the root causes.

Our recommendations remain largely unchanged from the previous year.

Slow response by management in improving internal controls

Detail of root cause

We identified the slow response by management (accounting officers/authorities and senior management) to our messages about addressing weaknesses in internal controls and the six risk areas as a root cause of poor audit outcomes at 73% of the 309 auditees that did not obtain clean audit opinions.

As shown in section 6.1 we found that the key controls at most of the auditees were not in place to support the preparation of quality financial statements and APFs and to ensure compliance with legislation. Role players such as the executive and coordinating institutions can positively contribute to an auditee's control environment. However, it is the responsibility of accounting officers and senior management to design and implement the controls and to ensure that they work effectively and consistently. As discussed in section 7, the accounting officers and senior management did not provide the level of assurance required and although the assurance slightly improved this first level of assurance remains lower than the other levels.

We assess the status of auditees' key controls periodically during the financial year and discuss the results with the accounting officers and key senior management officials. We specifically audit the six risk areas annually. We report all our audit findings in a management report that includes the root causes of the findings and our recommendations. Our message and the means of its delivery have been consistent for a number of years, but management's slow response to this message continues to hamper improvements in audit outcomes.

In our assessment, the slow response was prevalent at both departments (75%) and at public entities (72%), having become more prevalent at the latter, resulting in the overall increase of this particular root cause.

Our section on ministerial portfolios (section 9) and our provincial general reports provide details of commitments given and the progress thereon.

Recommendations

The following actions should be taken to eliminate slow response by management in improving internal controls as a root cause:

- Accounting officers and authorities should view the AGSA, internal audit units, audit committees and the risk management function as important partners in fulfilling their legislated responsibilities. Attention should be given to the reports of these assurance providers and there should be regular interactions with them.
- Accounting officers and authorities should ensure that senior management has action plans in place to address the internal control deficiencies identified by our reports as root causes of audit findings. The action plans should focus on the root causes of audit outcomes and not only on addressing specific findings, as this would prevent new or similar findings in future. Accounting officers and authorities should monitor the implementation of the plans.
- Executive authorities should hold accounting officers responsible for control weaknesses that are not addressed as it is an indication of neglect of their legislated duty to ensure there are effective, efficient and transparent systems of financial and risk management and internal control. In turn, accounting officers should ensure that senior managers are fulfilling their duties and address any negligence in this regard.
- The treasuries should intensify their current initiatives to support departments in improving their controls through guidance, interactions, capacity building and monitoring. Both treasuries and the departments responsible for public entities should also provide such support to public entities where it is apparent that the slow response by management is as a result of inadequate capacity and skills at management level.

Instability or vacancies in key positions

Detail of root cause

In our assessment instability and vacancies in key positions was a root cause at 46% of the 309 auditees that did not obtain clean audit opinions.

As discussed in section 5.1, the overall vacancy rates at auditees remain high, but in our view the vacancies and instability at the level of accounting officer, chief executive officer and chief financial officer are affecting the rate at which audit outcomes improve.

In our assessment, the impact of instability and vacancies is affecting audit outcomes at 55% of departments and to a lesser degree of public entities at 40%.

Recommendations

The following actions should be taken to eliminate instability or vacancies in key positions as a root cause:

- Executive authorities should appoint accounting officers in the departments where there are still vacancies and should endeavour to retain accounting officers in their positions for the period of their contract. Accounting authorities should commit to the same for chief executive officers.
- Accounting officers and authorities should fill the vacancies in senior management as soon as the position becomes vacant, with a maximum period of 12 months for a recruitment process. Particular attention should be paid to the appointment and retention of chief financial officers, heads of SCM and senior management responsible for strategic planning as well as monitoring and evaluation.
- Offices of the premier, the department of performance monitoring and evaluation, the treasuries and the departments responsible for the public entities should monitor vacancies and retention in key positions and provide support where needed.

Inadequate consequences for poor performance and transgressions

Detail of root cause

Inadequate consequences for poor performance and transgressions was a root cause of poor audit outcomes at 42% of the 309 auditees that did not obtain clean audit opinions (47% of the departments and 39% of the public entities).

Leaders and officials that deliberately or negligently ignore their duties and disobey legislation should be decisively dealt with through performance management and by enforcing the legislated consequences for transgressions. If they are not held accountable for their actions, the perception is created that such behaviour and its results are acceptable and tolerated.

The 2014-15 audits again confirmed weaknesses in the performance management of senior management. The inadequate response to the SCM transgressions, possible fraud and financial misconduct and unauthorised, irregular as well as fruitless and wasteful expenditure clearly shows a lack of consequences for transgressions. Section 5.1 includes more information in this regard.

Recommendations

The following actions should be taken to eliminate inadequate consequences for poor performance and transgressions as a root cause:

- Accounting officers and authorities should ensure that findings on compliance are investigated to determine whether there are indicators of financial misconduct or misconduct in the SCM processes, followed by disciplinary hearings where misconduct was confirmed. All unauthorised, irregular as well as fruitless and wasteful expenditure should also be investigated promptly to determine whether such expenditure should be recovered from the responsible official.
- To improve the performance and productivity of officials, the leadership should set the tone by implementing sound performance management processes, evaluating and monitoring performance, and consistently demonstrating that poor performance has consequences.
- Accounting officers and authorities, executive authorities and senior managers should demonstrate the importance of integrity and ethical values through actions and behaviour, and establish expectations for standards of conduct. The leadership should also ensure that deviations from expected standards are identified and addressed in a timely manner.