AUDITOR-GENERAL
SOUTH AFRICA

PFMA 2011-12

The drivers of internal control: Information technology management as a driver of audit outcomes

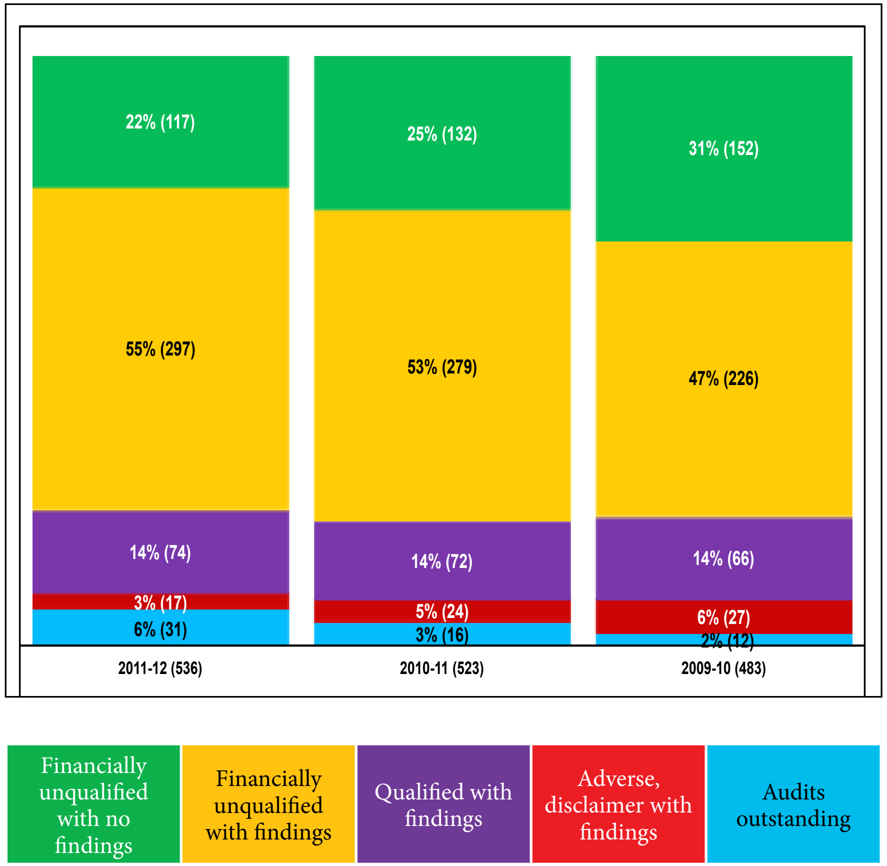
CONSOLIDATED GENERAL REPORT on NATIONAL and PROVINCIAL audit outcomes

Our reputation promise/mission

The Auditor-General of South Africa (AGSA) has a constitutional mandate and,
as the Supreme Audit Institution (SAI) of South Africa,
it exists to strengthen our country's democracy by enabling oversight,
accountability and governance in the
public sector through auditing, thereby building public confidence.

FOREWORD

Slow progress towards clean audits with slightly more regressions than improvements



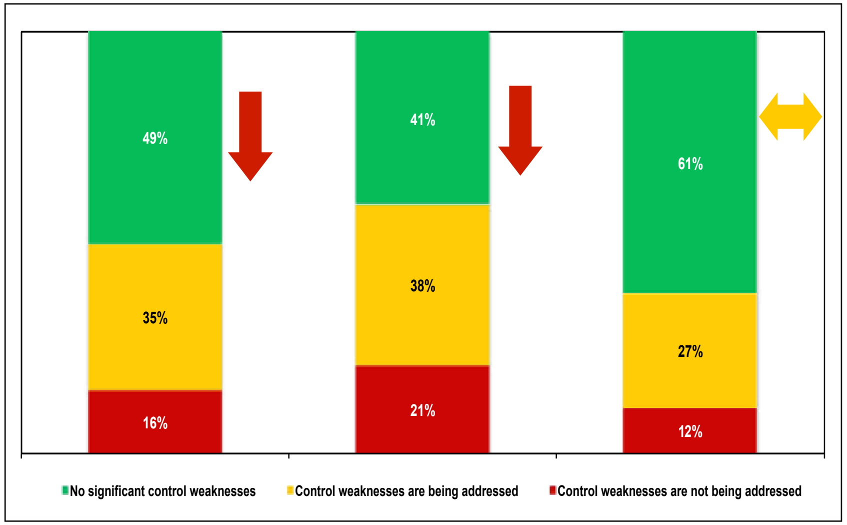
Limited progress made in addressing five key risk areas and regression in overall status of key controls

5 risk areas

Supply chain management	Predetermined objectives	HR	IT controls	Material mistakes in AFS submitted for audit
Minimal improvement	Improvement	Unchanged	Unchanged	Unchanged

Key controls

Leadership	Financial and performance management	Governance

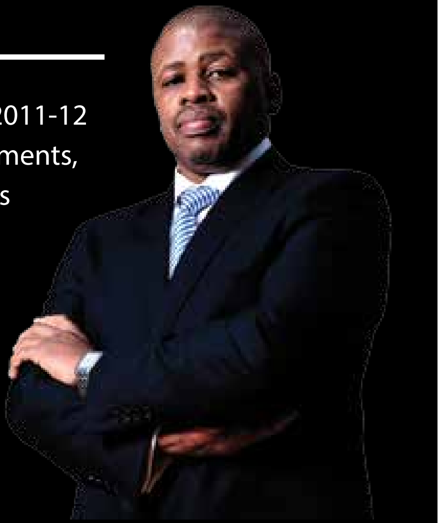


⬇	Regression	⟷	Unchanged

Pervasive root causes

- Vacancies in key positions, leadership instability and ineffective performance management
- Internal controls not effective – checks and balances not performed
- Not all role players are providing the level of assurance required

FOREWORD



It is a pleasure to present to Parliament my 2011-12 general report on audit outcomes of departments, legislatures, public entities and other entities in the national and provincial spheres of government.

In response to the 2010-11 audit outcomes, commitments were made by the executive and oversight bodies to intensify their efforts in bringing positive change within the administration.

Despite my expectation that these commitments would drive improvements towards clean audits, the audit outcomes for the year show a general stagnant trend, with less than a quarter of auditees obtaining clean audit opinions and 52 not able to sustain their prior year clean audit opinion. My report shows that many leaders did not own and drive these commitments, so the commitments are left to flounder until the next audit starts. In this regard, I single out two significant commitments made a year ago:

- The executive committed to meet with my office quarterly for at least an hour. About 78% of them have made time at least three times in the past year to meet and share the results of our assessment of the risks and controls and to consider the status of commitments made and make new commitments. Although the engagements were well received, only small movements in audit outcomes can be seen. This was due to frequent leadership changes resulting in disruption in the implementation of commitments, our message being ignored, or our conversation not being compelling and persuasive enough. We therefore undertake to continue with the quarterly engagements, but with greater emphasis on quality conversations leading to increased impact.
- Parliament and legislatures committed to improve the collaboration between their respective public accounts committees and portfolio committees. We have yet to see more concentrated efforts in this regard as an uncoordinated approach will continue to weaken the effectiveness of oversight.

Of special concern is the increase in auditees with material findings on non-compliance with legislation, bringing it to 74%. Even though I have stressed for the past three years the urgent need to address the quality of the financial statements submitted for audit and weaknesses in supply chain management, human resource management and information technology controls, there has been minimal improvement.

The usefulness and reliability of the annual performance reports continue to improve, which is gratifying. I am now able to make a clearer assessment of service delivery risks but not to the full extent necessary (as some key departments responsible for national outcomes, such as those in the health, education and human settlement sectors, continue to have material shortcomings). Based on the annual performance reports, about 42% of auditees achieved 80% or fewer of their planned service delivery targets, while some departments had significantly underspent their conditional grants and capital budgets. My report further highlights risks to the financial health of national and provincial government flowing from poor budget management, cash and debtors management of departments and the financial management of some public entities. These indicators reflect that the fiscus could be placed under further pressure if such risks are not addressed.

In this general report, I raise three areas that require corrective steps by those charged with governance to achieve improvements in the audit outcomes:

- **Vacancies in key positions** and **instability in leadership** positions affect the pace of sustainable improvements. **Ineffective performance management** is evident at some auditees, which means that officials who perform poorly are not dealt with decisively. A concerted effort is required to address the challenges in human resource capacity and productivity.

- **Effective internal controls** to prevent, detect and correct non-compliance with legislation and mistakes in the financial and performance reports are lacking. Overall the effectiveness of key controls has regressed, as they were not designed and implemented in a sustainable manner. Checks and balances for all key processes, monthly reporting and validation processes to ensure the credibility of all management information are basic controls which skilled professional should be able to implement.
- Government should be monitored in a thorough, diligent and collaborative manner. My office only provides independent assurance on the credibility of financial and performance information and compliance with selected legislation. We are not the only **provider of assurance** to the citizens that government is delivering services in a responsible and accountable manner. The monitoring functions vested in **senior management, accounting officers, internal audit, audit committees and executive authorities** should be better exercised so that audit outcomes and service delivery issues are dealt with through self-monitoring, while audit provides an external validation. The **treasuries, offices of the premiers, public service administration and other coordinating/monitoring institutions** should fulfil their role envisaged in legislation to guide, support, coordinate and monitor government. The **legislatures and Parliament** should be scrupulous and courageous in performing their oversight function in order to make an impact on clean administration. My assessment (detailed in this report) is that not all of these role players are providing the level of assurance required to create the momentum towards improve audit outcomes.

A common reaction to the audit outcomes is the question posed by many about the need for officials to be accountable, and for there to be consequences for poor performance, misappropriation of state resources and fraud. In response, we have highlighted in a separate booklet, the range of legislation at the government's disposal that enables remedies to be applied where there has been transgression. These must be used where necessary to reverse the culture of "business-as-usual". It is my assessment that the full power of the law is yet to be activated, leading to commentators asking "What can be done?" or saying "There are no consequences". Highlighting these remedies provides a starting point for our responsible leaders and the relevant legislatures and departments to take action. All parties have to play their part.

Although progress towards clean audits is slow, I am encouraged by examples of commitments by leaders and officials which translated into improved audit outcomes and I am confident similar results can be achieved by all auditees. In conjunction with various key role players, my office has provided input towards the development of solutions to the challenges highlighted in this report, and will in future share assessments of progress in joint sessions with the Head of Government Business and Parliament and through similar engagements in the provinces.

It is through all our efforts and the work of auditors that we will contribute towards strengthening our democracy through auditing.

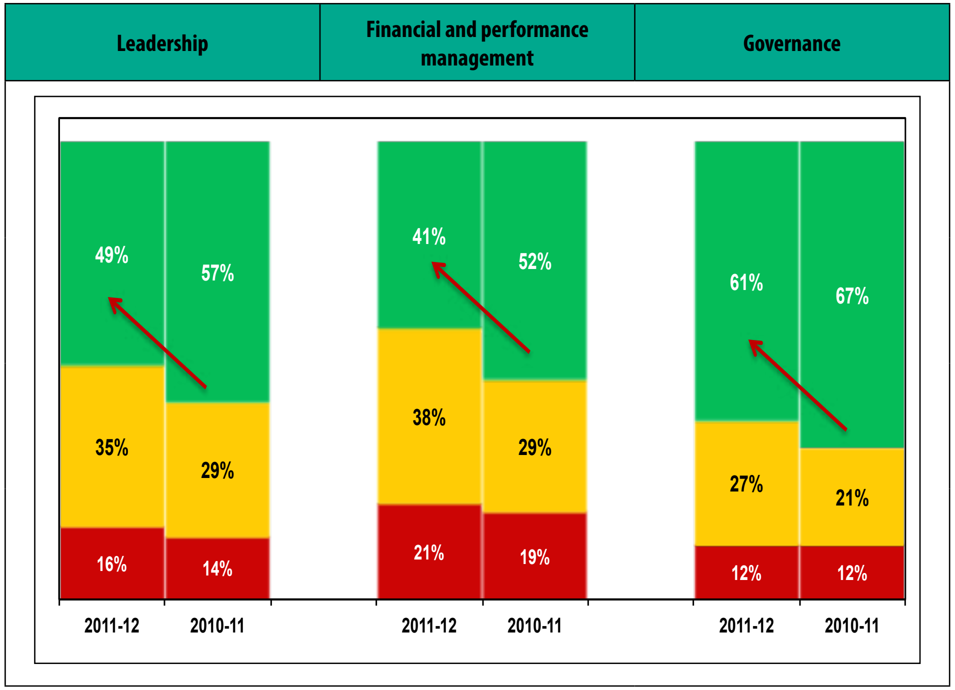
Auditor-General

Auditor-General
Pretoria
March 2013

THE DRIVERS OF INTERNAL CONTROL

AUDITEES' SYSTEMS OF INTERNAL CONTROL

3.1 THE DRIVERS OF INTERNAL CONTROL



Internal control driver	Objectives and impacted on by internal control driver		
	Financial management and reporting	Service delivery planning and reporting	Compliance with laws and regulations
Leadership	49% 35% 16%	54% 30% 16%	51% 33% 16%
Financial and performance management	41% 38% 21%	50% 29% 21%	49% 31% 20%
Governance	61% 27% 12%	61% 26% 13%	60% 29% 11%

🟩 Good 🟨 Causing concerns 🟥 Intervention required

Regression ↖

This section of the general report identifies the drivers of audit outcomes under the following headings:

- Significant deficiencies in auditees' systems of internal control and the drivers thereof (section 3.1)
- Effective human resource management as driver of audit outcomes (section 3.2)
- The use of consultants by some national departments (section 3.3)
- Information technology management as driver of audit outcomes (section 3.4)
- The effectiveness of audit committees and internal audit units (section 3. 5).

A key responsibility of accounting officers/authorities and other officials is to implement and maintain effective and efficient systems of internal control. As part of the audits, the auditees' system of internal control is assessed to determine its effectiveness in ensuring reliable financial and performance reporting and compliance with laws and regulations, which in turn will result in a clean audit. For purposes of focusing corrective action, the principles of the different components of internal control, termed drivers of internal control, have been categorised under leadership, finance and performance management and governance.

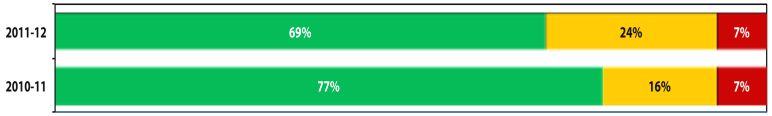
The figure alongside provides the overall assessment of these drivers at the time of the audit, based on significant deficiencies identified in internal control which resulted in material misstatements (corrected and uncorrected) in financial statements and also in performance reports as well as findings on compliance with laws and regulations. The following broad areas of concern are highlighted.

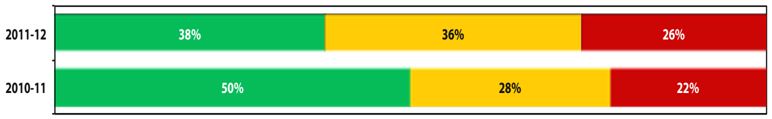
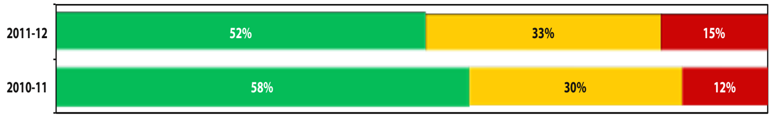
🟥	The overall reduction in the number of auditees whose drivers were assessed as being 'good' at the conclusion of the 2010-11 audits.
🟥	The overall increase in the number of auditees requiring intervention in controls related to financial and performance management
🟥	The impact of the combined deficiencies in leadership, financial and performance management and governance on all three facets of the audit outcomes: (i) financial statements, (ii) reporting against PDOs (service delivery reporting) as well as on (iii) compliance with laws and regulations.

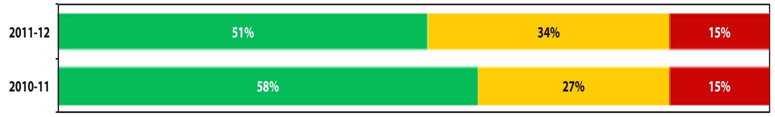
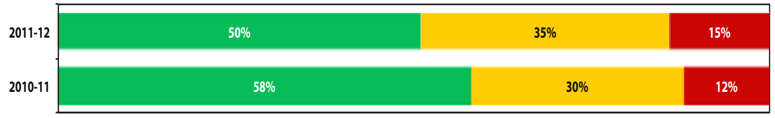
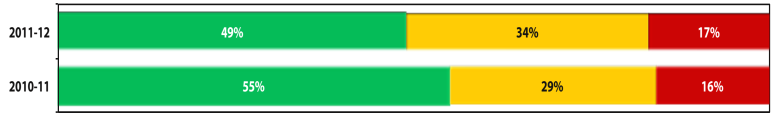
Root causes and recommended best practices are analysed in more detail under section 2.2 (financial statement qualifications), 2.3 (PDO findings) and 2.4 (findings on non-compliance with laws and regulations).

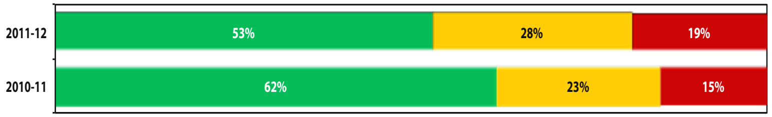
The status of the **internal *control* elements** at March 2012, underlying leadership, financial and performance management and governance and movements in the implementation thereof, is presented in the following table, indicating overall deteriorations (red arrows) or overall unchanged status from the previous financial year (sideway arrows) for departments and public entities.

Table 17: The status of and movements in the internal control elements underlying leadership, financial and performance management

<table>
<tr><th>Driver no. 1: Leadership</th><th>Departments</th><th>Assessment of driver (all auditees)</th><th>Public entities</th></tr>
<tr><td>Provide effective leadership based on a culture of honesty, ethical business practices and good governance, protecting and enhancing the interests of the entity.</td><td>⬇</td><td> </td><td>⬌</td></tr>
<tr><td colspan="4">The majority of auditees were assessed to have committed and ethical leadership. However, instability in political leadership and ineffective administrative leadership have negatively affected the audit outcomes of some auditees. Neither administrative nor political leadership adequately addressed the matters that prevent auditees from progressing towards clean audits. The weaknesses in leadership practices at some auditees include the following:
• Failure to implement formal codes of conduct and periodically communicate to officials their existence and continued applicability.
• Failure to monitor the performance of key officials relating to the maintenance of adequate systems of internal control that ensure credible monthly financial reporting, reliable reporting against PDOs and compliance with laws and regulations.
• Failure to establish clear lines of accountability.
• Corrective/disciplinary action not taken against key officials for misconduct.
• Failure to honour commitments made for interventions following the 2010-11 audit outcomes.
• The awarding of contracts to employees, close family members of employees and other state officials.</td></tr>
</table>

Driver no. 1: Leadership	Departments	Assessment of driver (all auditees)	Public entities
Exercise oversight responsibility regarding financial and performance reporting and compliance with laws and regulations and related internal controls.	⬇		⬇
Leadership at auditees who failed to make progress and those whose outcomes have regressed has not effectively exercised their oversight responsibility with regard to financial and performance reporting and compliance with applicable laws and regulations. Lapses in effective oversight include the following: • Not exerting a positive influence on the control environment. • Not ensuring that auditees appoint suitably qualified staff to perform essential duties related to financial and performance reporting. • Not periodically reviewing progress made by management in addressing external audit findings. • Not monitoring controls. • Not addressing the root causes of repeated qualifications of financial statements, findings on reporting against PDOs as well as findings on non-compliance with laws and regulations. • No insisting (i) on receiving credible monthly financial statements, (ii) that proper accounting records be maintained, (iii) that key reconciliations are periodically prepared, and (iv) the accuracy of reported information is independently verified.			
Implement effective human resource management to ensure that adequate and sufficiently skilled resources are in place and that performance is monitored.	⬇		⬇
An assessment of findings arising from the audit of human resource management is presented in section 3.2 of this general report			

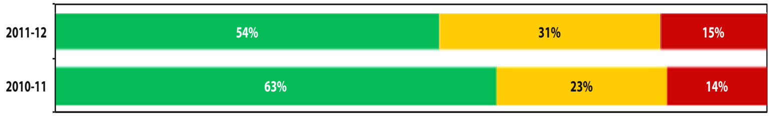
<table>
<tr><th>Driver no. 1: Leadership</th><th>Departments</th><th>Assessment of driver (all auditees)</th><th>Public entities</th></tr>
<tr><td>Establish and communicate policies and procedures to enable and support an understanding and execution of internal control objectives, processes and responsibilities.</td><td>↓</td><td> </td><td>↓</td></tr>
<tr><td colspan="4">Policies and procedures to address areas of risk, to achieve desired internal control objectives and to guide the operations of auditees still require improvement at many auditees. Matters that specifically need to be addressed include the following:
• The effective implementation of documented policies and procedures.
• Many auditees have not put in place policies specifically providing guidelines and directives for the collection, processing and validation of performance information.
• Policies and procedures are not in place to ensure compliance with the laws and regulations.
• Auditees whose policies and procedures are still in draft should prioritise their finalisation and monitor compliance once approved. .</td></tr>
<tr><td>Develop and monitor the implementation of action plans to address internal control deficiencies.</td><td>↓</td><td> </td><td>↓</td></tr>
<tr><td colspan="4">Specific action plans are required to address internal control deficiencies and improve audit outcomes. Matters requiring attention include the following:
• Setting action plans to specifically address the external and internal audit findings. Some action plans did not address the root causes of audit findings and therefore did not prevent repeat findings.
• Staff members were not assigned responsibility to carry out these action plans.
• Ineffective monitoring to ensure that the responsibilities assigned were carried out effectively and consistently.
• Some auditees' action plans were developed too late in the financial year to resolve matters by year-end.
• Action plans do not address all three facets of audit outcomes, namely qualifications, findings on PDO reporting and compliance with laws and regulations.</td></tr>
<tr><td>Develop and monitor the implementation of action plans to address internal control deficiencies in the IT environment. Establish an IT governance framework that supports and enables the business, delivers value and improves performance.</td><td>↔</td><td> </td><td>↓</td></tr>
<tr><td colspan="4"><b>An assessment of information technology controls is presented in section 3.3 of this general report</b></td></tr>
</table>

Driver no. 2: Financial and performance management	**Departments**	**Assessment of driver (all auditees)**	**Public entities**
Implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.	⬇		⬇

Proper record keeping is an essential step towards achieving clean audit outcomes as it ensures that the information reported can be substantiated and verified. It also empowers senior management to hold staff accountable for their actions. An adequate system of record keeping requires that senior management establish adequately developed and communicated policies to ensure that staff align their actions with the entity's objectives. A key objective of maintaining a formal and reliable system of record keeping is to have documentation readily available when requested.

Most auditees' financial and performance systems have not yet reached the level of maturity where information is centrally available and evidence to support major decisions is readily available. The root causes include the following:

- A lack of document management policies.
- Poor monitoring of those policies by management where policies do exist.
- A lack of willingness by leadership to implement those commitments that were made to specifically address the recurring instances of missing and incomplete supporting information.
- A lack of management of documentation to support the reported performance against PDO.

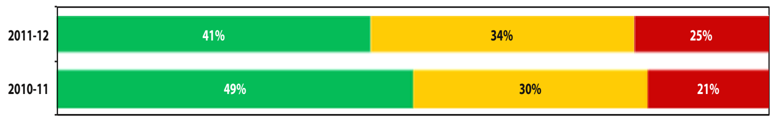
Driver no. 2: Financial and performance management	**Departments**	**Assessment of driver (all auditees)**	**Public entities**
Implement controls over daily and monthly processing and reconciling of transactions.	⬇		⬇

Driver no. 2: Financial and performance management	Departments	Assessment of driver (all auditees)	Public entities

Auditees that improved or sustained their audit outcomes were found to effectively monitor daily and monthly processing and reconciling of transactions. Auditees that improved on reconciliation processes and reconstruction of fixed assets register were able to resolve audit qualifications. Monthly reconciliations and clearing of suspense accounts provide the platform for reliable in-year financial reporting and the early detection of errors in and omissions from financial and performance reporting.

Poor and deteriorating controls which negatively impacted on audit outcomes included the following:

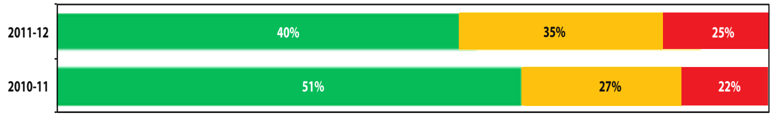
- Key controls were not reviewed and monitored on a daily, weekly and monthly basis.
- Assets were not verified at least on a quarterly basis to ensure that asset registers are reliable, which resulted in errors being detected only when an audit is performed.
- Auditees did not ensure that controls such as the following are in place:
  - Daily capturing of financial transactions, supervisory reviews of captured information and independent monthly reconciliation of key accounts.
  - Collection of performance information at intervals that are appropriate for monitoring of set service delivery targets and milestones and validation of recorded information.
  - Management of contracts and the commitments relating to such contracts.
  - Confirmation that legislative requirements and policies have been complied with prior to initiating transactions.

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

Only when the in-year preparation and independent review of financial statements and performance information become an established practice will the quality of financial statements submitted for audit significantly improve and findings resulting from material misstatements in financial statements and performance reports be eliminated.

The following matters contribute to poor audit outcomes due to errors in and omission of information which cannot all be corrected when the annual audit has commenced, resulting in qualifications or material PDO findings:

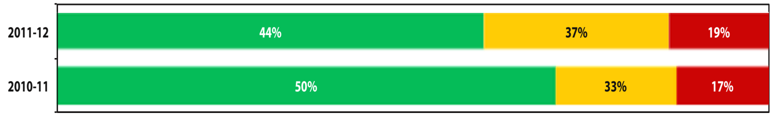
- The practice of regular internal reporting is not fully embedded at most auditees to ensure self-monitoring, thereby reducing the likelihood of producing financial statements that attract qualifications when audited, or findings on the usefulness and/or reliability of performance information.
- Leadership does not insist on receiving in-year financial and performance reports that are independently validated, as well as reports on legislative requirements having being met.
- Finance staff lack an adequate understanding of the reporting framework, resulting in them not being able to draft the required disclosure notes to the financial statements.
- Over-reliance on consultants to assist auditees in achieving an unqualified audit opinion.

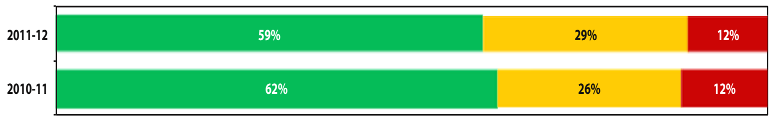
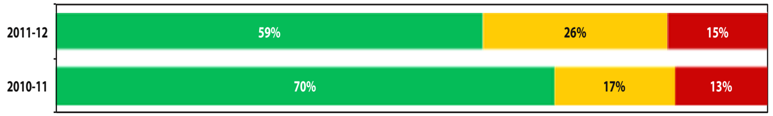
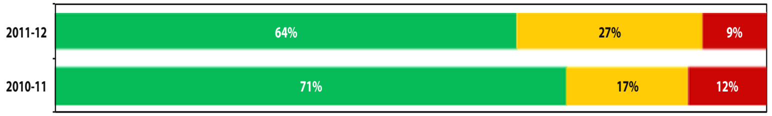
Driver no. 2: Financial and performance management	Departments	Assessment of driver (all auditees)	Public entities
Review and monitor compliance with applicable laws and regulations.	↓		↓

Management should conduct regular monitoring to ensure that appropriate controls are in place with a view to consistent compliance with all applicable laws and regulations as a significant number of auditees remain in the 'unqualified with findings on non-compliance' category. Leadership should focus on the regular monitoring of common areas of non-compliance and the effective implementation of checklists to ensure compliance before transactions are concluded and not after payments have been made.

Findings on non-compliance with applicable laws and regulations are the result of matters that commonly include the following:

- Management and governance structures have not established their own processes to identify all existing legislation applicable to their departments and public entities.
- Instances that point to a deliberate disregard for laws and regulations.
- Certain cases where management fails to demonstrate any commitment to ensure compliance with the relevant laws and regulations.
- There appears to be no appreciable consequences for officials who fail to comply with laws and regulations to which departments and public entities are subject or for officials who fail to discharge their legislated duties.
- While many auditees do have policies and procedures in place to monitor compliance with laws and regulations, monitoring should take place at more frequent intervals, such as on a monthly basis, by dedicated/designated staff members with a view to detecting, or preferably preventing, non-compliance.

Design and implement formal controls over IT systems to ensure the reliability of the systems and the availability, accuracy and protection of information and to address application systems susceptible to compromised data integrity (Information systems).	↔		↓

Driver no. 3: Governance	Departments	Assessment of driver (all auditees)	Public entities
Implement appropriate risk management activities to ensure that regular risk assessments, including consideration of IT risks and fraud prevention, are conducted and that a risk strategy to address the risks is developed and monitored.	↔		↓
Risk management is the practice of identifying, assessing and prioritising risks and developing risk management plans which are essential elements in the review of the design and implementation of sound internal controls to achieve good governance and accountability in respect of financial reporting and reporting on achievements against PDOs (service delivery) Risk management activities that require attention from leadership, management and governance structures of departments and public entities include the following: • A lack of risk assessments and risk management strategies that sufficiently cover financial reporting, reporting on achievements against PDOs and consistent compliance with applicable laws and regulations. • IT risk plans and fraud prevention plans were inadequately implemented. • Risk management strategies were developed but not appropriately implemented and monitored. • A significant number of auditees could not provide sufficient adequate evidence that their IT risks such business continuity, IT governance and user access management are well managed. This has a significant impact on auditees' ability to achieve excellent public administration as most transactions are now initiated through a computer, processed and reported by computerised application. • Auditees' risk assessment results do not inform the work plans of internal audit and the agendas of audit committees.			
Section 3.5 of this report provides an assessment of the effectiveness of internal audit units			
Ensure that an adequately resourced and functioning internal audit unit is in place that identifies internal control deficiencies and recommends corrective action effectively.	↓		↓
Section 3.5 of this report provides an assessment of the effectiveness of audit committees			
Ensure that the audit committee promotes accountability and service delivery through evaluating and monitoring responses to risks and providing oversight of the effectiveness of the internal control environment, including financial and performance reporting and compliance with laws and regulations.	↓		↔

THE DRIVERS OF INTERNAL CONTROL: INFORMATION TECHNOLOGY MANAGEMENT AS A DRIVER OF AUDIT OUTCOMES

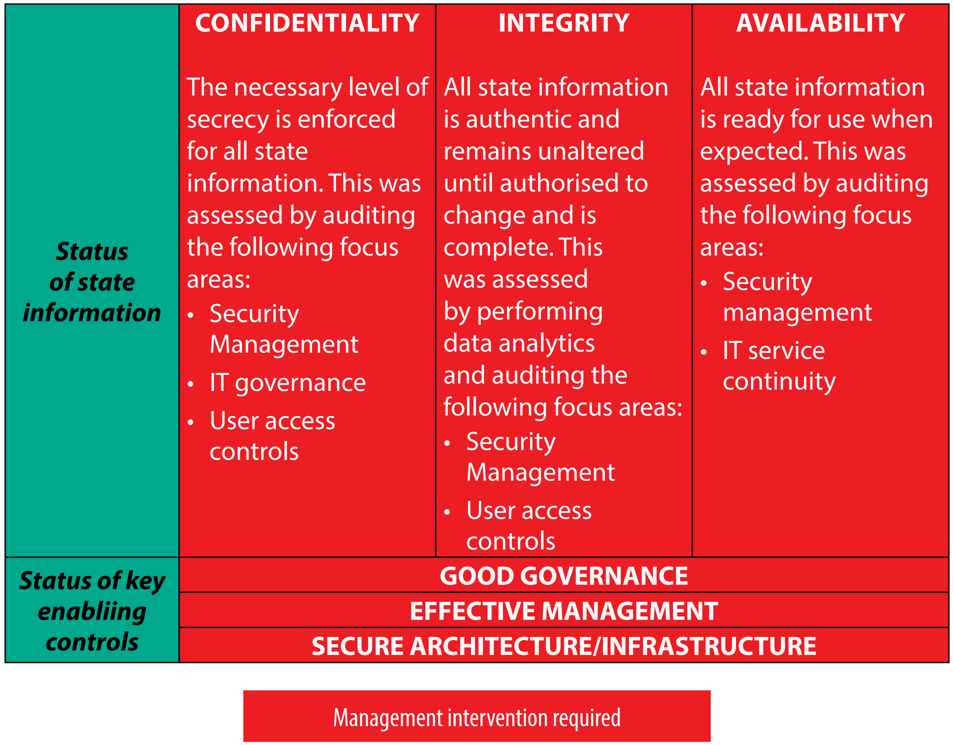
3.4 INFORMATION TECHNOLOGY MANAGEMENT AS A KEY DRIVER OF AUDIT OUTCOMES

Information technology (IT) controls that ensure the confidentiality, integrity and availability of data need to be properly designed and implemented and have to function effectively to maintain the operational integrity of the state, enable service delivery and promote national security.

It is thus essential for good IT governance, effective IT management and a secure IT architecture / infrastructure to be in place.

The following diagram provides a consolidated view of the status of IT across national departments and public entities, based on our audit outcomes:

Figure 23: Status of information technology across national departments and public entities

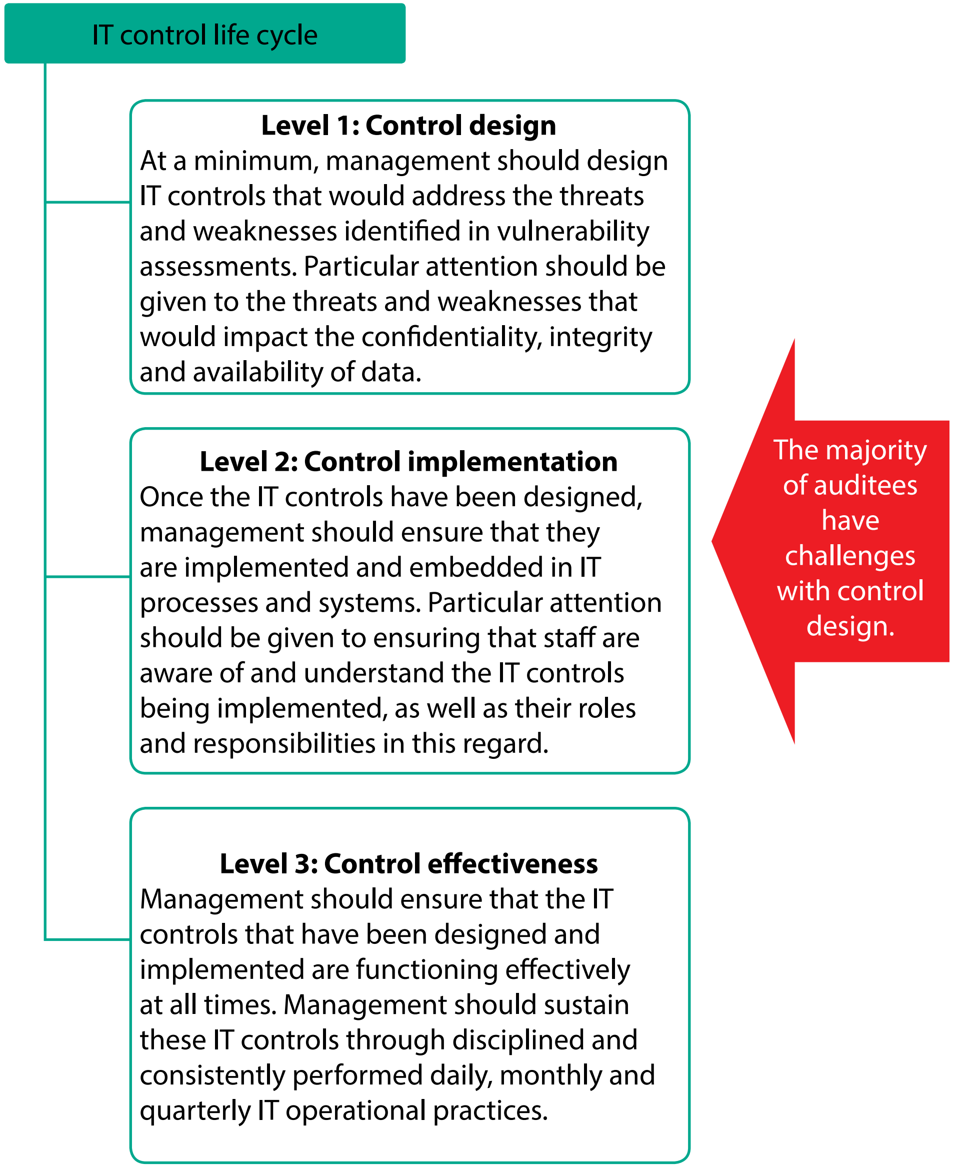


	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Status of state information	🟥 The necessary level of secrecy is enforced for all state information. This was assessed by auditing the following focus areas: • Security Management • IT governance • User access controls	🟥 All state information is authentic and remains unaltered until authorised to change and is complete. This was assessed by performing data analytics and auditing the following focus areas: • Security Management • User access controls	🟥 All state information is ready for use when expected. This was assessed by auditing the following focus areas: • Security management • IT service continuity
Status of key enabliing controls	🟥 **GOOD GOVERNANCE**		
	🟥 **EFFECTIVE MANAGEMENT**		
	🟥 **SECURE ARCHITECTURE/INFRASTRUCTURE**		

🟥 Management intervention required

IT controls typically move through a life cycle that includes the three stages of design, implementation and effectiveness.

Figure 24: Typical information technology control life cycle



IT control life cycle

Level 1: Control design
At a minimum, management should design IT controls that would address the threats and weaknesses identified in vulnerability assessments. Particular attention should be given to the threats and weaknesses that would impact the confidentiality, integrity and availability of data.

Level 2: Control implementation
Once the IT controls have been designed, management should ensure that they are implemented and embedded in IT processes and systems. Particular attention should be given to ensuring that staff are aware of and understand the IT controls being implemented, as well as their roles and responsibilities in this regard.

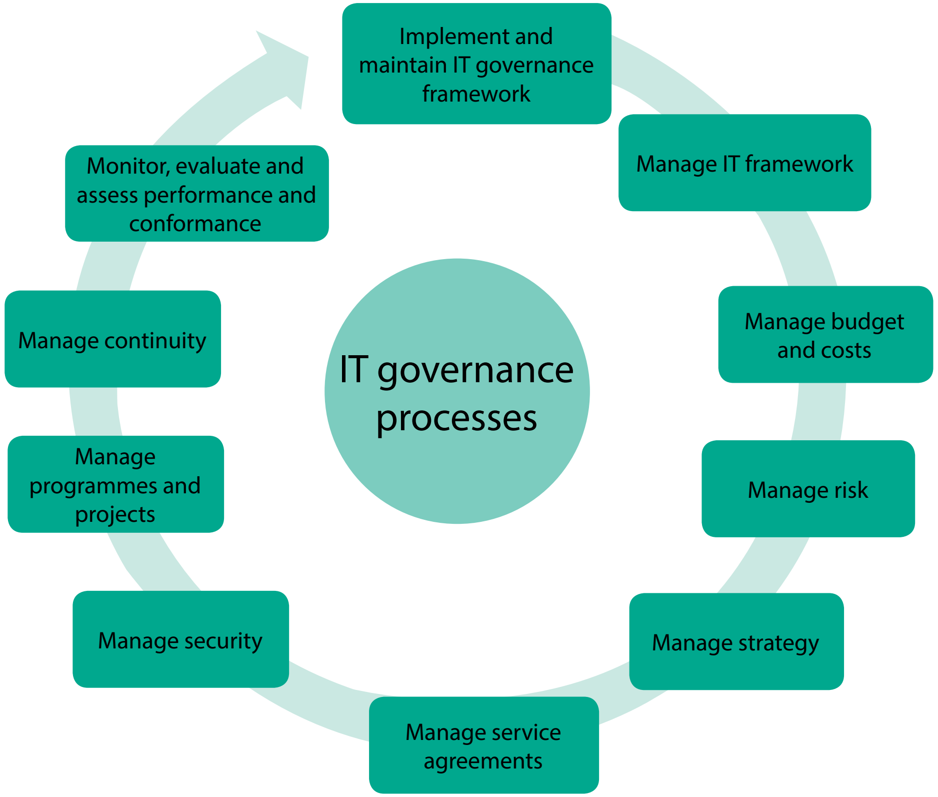
Level 3: Control effectiveness
Management should ensure that the IT controls that have been designed and implemented are functioning effectively at all times. Management should sustain these IT controls through disciplined and consistently performed daily, monthly and quarterly IT operational practices.

The majority of auditees have challenges with control design.

3.4.1 Information technology governance

Delays in the approval, roll-out and implementation of a government-wide IT governance framework resulted in the IT governance processes depicted in the diagram below not being implemented effectively in the majority of national departments and entities. These governance processes are based on the framework endorsed by the Department of Public Service and Administration (DPSA) and the Government Information Technology Officers Council (GITOC).

Figure 25: Information technology governance processes



IT governance processes

Implement and maintain IT governance framework

Manage IT framework

Manage budget and costs

Manage risk

Manage strategy

Manage service agreements

Manage security

Manage programmes and projects

Manage continuity

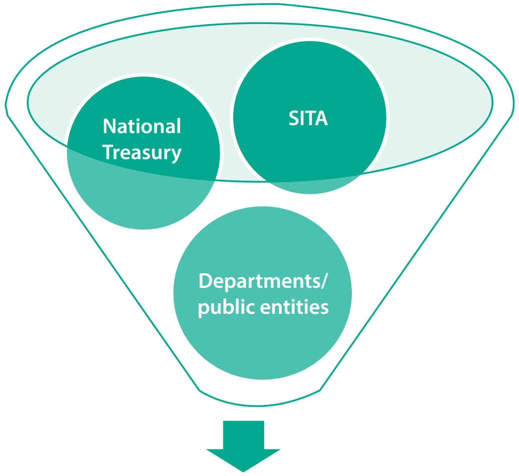
Monitor, evaluate and assess performance and conformance

3.4.2 Summary of weaknesses identified in the management of financial information systems

The transversal financial systems used by national government departments, i.e. the Basic Accounting System (BAS), the Personnel and Salary System (Persal) and the Logistical Information System (Logis), are hosted by the State Information Technology Agency (SITA). SITA is responsible for establishing and maintaining security controls over the network that connects these systems with the national government departments. SITA also ensures that information from the departments that is processed on these systems is centrally backed up. The National Treasury (NT) is responsible for ensuring that programmatic changes to these systems are managed and controlled. In contrast, public entities utilise various financial systems and manage these on their own with no intervention from either NT or SITA.

Adequate coordination between SITA, NT and government departments and public entities would contribute towards ensuring a secure IT environment for financial systems.

Figure 26: Key role players in ensuring a secure information technology environment



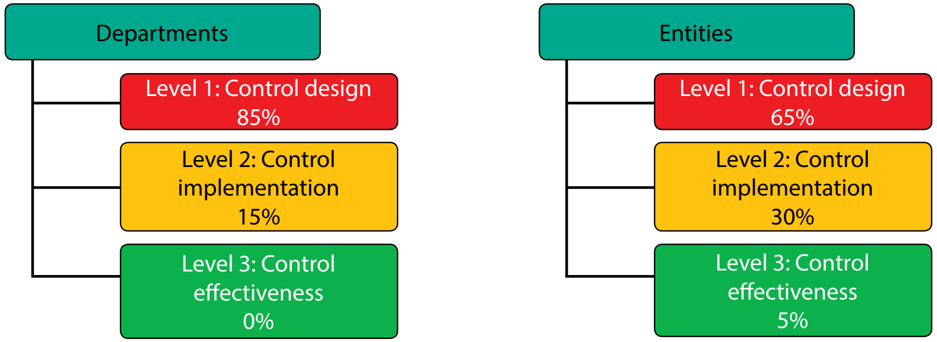
Secure financial systems

IT controls were assessed at 40 national departments and 109 public entities. An analysis of the audit outcomes indicated that the majority of departments and entities experienced challenges with the design and implementation of IT controls that provide assurance of the confidentiality, integrity and availability of financial information.

Weaknesses specific to focus areas have been summarised below:

3.4.2.1 Program change management

Figure 27: Control weaknesses in program change management


Departments
Level 1: Control design 85%
Level 2: Control implementation 15%
Level 3: Control effectiveness 0%
Entities
Level 1: Control design 65%
Level 2: Control implementation 30%
Level 3: Control effectiveness 5%

- ***National Treasury***

  Program and data change controls were adequately designed and implemented and operated effectively on the BAS and Logis systems. However, the controls governing the correction of personnel records on the Persal system were not adequately designed. The risk of unauthorised changes being made to personnel and financial information was compounded by inherent weaknesses such as the ageing technology of the transversal systems.

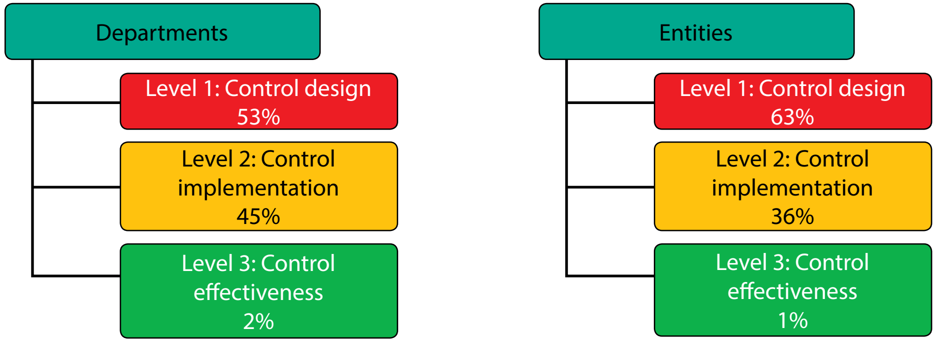
- ***Departments and entities***

  Program and data change controls for public entities were not adequately designed. As a result, changes were implemented that had not been approved or tested.

Inadequate segregation of duties stemming from programmers having permanent access to the live environments of the transversal and non-transversal systems at both departments and public entities resulted in management not always being empowered to ensure the integrity of personnel and financial information.

3.4.2.2 Security management

Figure 28: Control weaknesses in security management


Departments
Level 1: Control design 53%
Level 2: Control implementation 45%
Level 3: Control effectiveness 2%
Entities
Level 1: Control design 63%
Level 2: Control implementation 36%
Level 3: Control effectiveness 1%

- ***State Information Technology Agency***

Significant control deficiencies related to encryption, Internet security and firewall configurations were identified on SITA's network. These control deficiencies could impact on the security of the financial systems used by government departments.

Formal information security policies and standards had not been designed for the network infrastructure.

Information security responsibilities for the infrastructure that supports the network environment had also not been assigned to an information security officer.

The security measures were therefore inadequate to protect the confidentiality, integrity and availability of the financial, performance and personnel information stored by SITA on behalf of all government departments.

- ***Departments and entities***

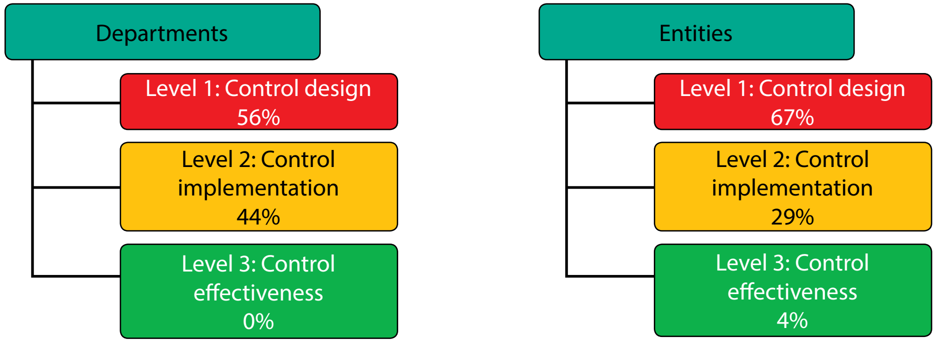
As a result of the lack of formally designed and implemented information security policies and standards, effective security controls were not in place, which gave rise to the following weaknesses:

- Firewalls were not securely configured.
- Antivirus software and patches were not updated.
- Password controls were not adequately configured.

The weak security control environment was in a number of instances exploited to gain unauthorised access.

3.4.2.3 User access management

Figure 29: Control weaknesses in user access management

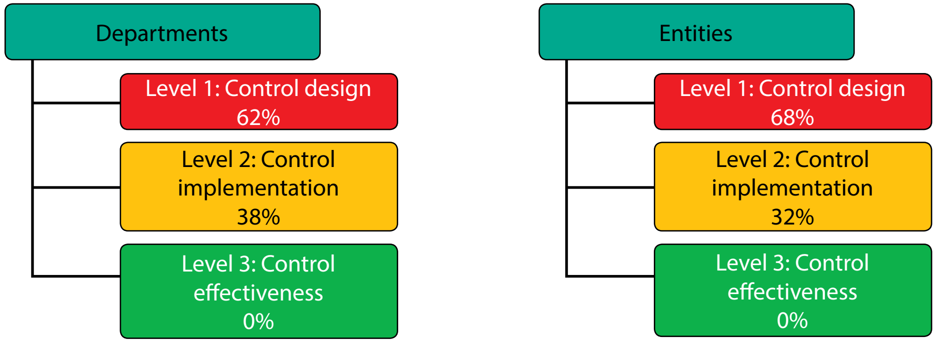

Departments
Level 1: Control design 56%
Level 2: Control implementation 44%
Level 3: Control effectiveness 0%
Entities
Level 1: Control design 67%
Level 2: Control implementation 29%
Level 3: Control effectiveness 4%

The lack of implementation of user access controls gave rise to the following weaknesses:

- Users who left organisations were not removed from systems in a timely manner.
- User access profiles used to initiate and approve financial and HR transactions were not continuously monitored to ensure that only authorised access would be given to users.
- Users were created on systems without supporting documentation.
- User passwords were reset without supporting documentation.
- System controller access that allowed a person to perform the above actions was not monitored to ensure that only authorised transactions were performed.

3.4.2.4 Information technology service continuity

Figure 30: Control weaknesses in information technology service continuity


Departments
Level 1: Control design 62%
Level 2: Control implementation 38%
Level 3: Control effectiveness 0%
Entities
Level 1: Control design 68%
Level 2: Control implementation 32%
Level 3: Control effectiveness 0%

- Business continuity plans had not been designed to ensure that all critical business processes supported by IT systems would be identified and included in a recovery plan. This gave rise to the risk of misalignment between business expectations and IT recovery processes, as departments and public entities might not be able to recover information systems services to enable the timely resumption of business in the event of a business disruption and IT disaster. This risk was elevated by the lack of disaster recovery testing that would establish recovery capabilities.
- Disaster recovery plans that could be invoked to recover IT systems to a normal operating state in the event of a disaster had not been documented for departments and entities. The risk of data loss was further increased by the inconsistent performance of recovery disciplines, such as daily backups, off-site storage and periodic data restoration tests. For entities, the lack of a centralised disaster recovery facility, such as that provided by SITA for the departments, increased the risk of business continuity and data recovery not being possible in the event of a disaster.

3.4.3 Project risks in developing or implementing major systems in government

Trends were noted in entities and legislatures embarking on the implementation of Enterprise Resource Planning (ERP) systems from vendors such as Oracle and SAP. While the implementation of these systems is not necessarily problematic, the status of the current IT environment elevates certain key risks related to their deployment, as the following examples will illustrate.

Figure 31: Examples of information technology project risks elevated by the status of the current environment

Pre-initiation

- Not having a business case, or having a poorly developed business case, could result in questionable project decisions, intended business objectives not being met, incorrect solution selection and inaccurate budgeting. Further, there is a risk of functionality in existing systems being duplicated.
- The lack of engagement with users in defining their requirements could result in an inadequate system that does not meet all business needs.
- The lack of appropriate executive and/or senior leadership involvement from the outset could result in poor oversight and management of the project.

Initiation

- Not having a project management and governance framework, or having one that is inadequate, may result in poor management and control of project deliverables and risks.
- Inadeqaute stakeholder identification and engagement could result in unnecessary delays during subsequent project implementation phases.

Planning

- A lack of input from subject matter experts/users could result in inadequate planning, poor technology selection and inadequate management of critical success factors related to project costs, quality and schedule.
- Risks related to implementation scope, procurement, human resources, communication, information security, end-user acceptance, integration and change management may also be poorly managed.

Execution

- Insufficient resources and/or a lack of suitably skilled resources could result in dependency on consultants and delays in execution.

Monitoring and control

- Ineffective project leadership and governance, a lack of continuous risk and internal audit assurance oversight and a lack of compliance with established project implementation disciplines could result in projects not meeting business objectives.
- Poor contract management could result in project delays, budget overruns, inferior quality and a lack of proper scope management.

Closing and operations

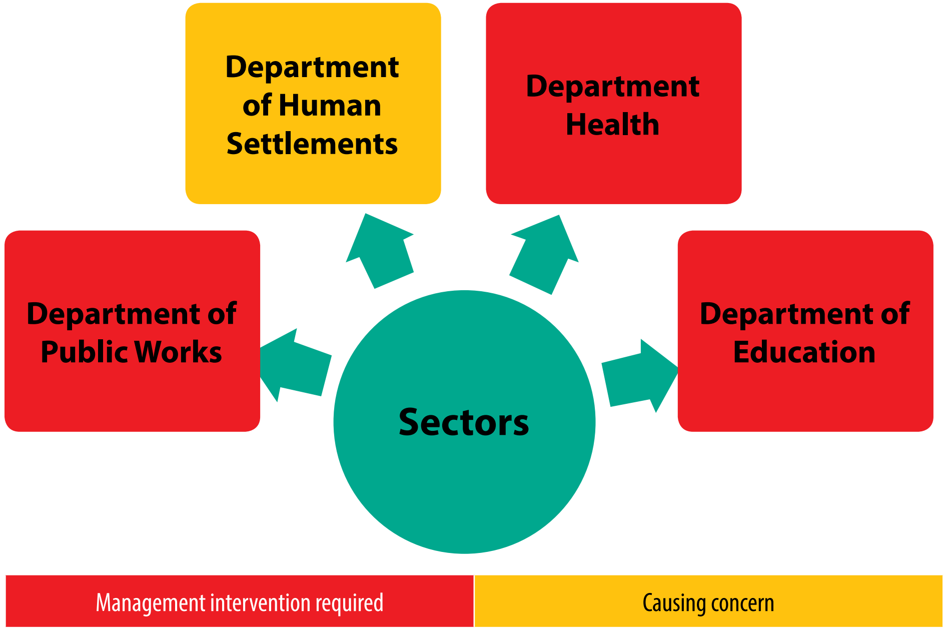
- Inadequately planned project handover processes could result in operations teams not having the capability or capacity to support the system once it has been implemented.
- Inadequate operations and maintenance planning could impact the sustainability of the solution and long-term benefits realisation.

3.4.4 Summary of identified weaknesses in the management of performance information systems

Framework 86 of 2007 was compiled by the National Treasury for managing programme performance information. According to this framework, the national departments have the overall responsibility for designing IT controls to govern the systems used by the provincial departments for reporting on the achievement of predetermined objectives. IT controls that ensure the confidentiality, integrity and availability of performance data need to be properly designed and implemented and have to function effectively to maintain the operational integrity of the state and enable service delivery.

The following diagram provides a consolidated view of the status of performance information systems for the sectors audited:

Figure 32: Status of performance information systems controls


Department of Human Settlements
Department Health
Department of Public Works
Sectors
Department of Education
Management intervention required
Causing concern

3.4.4.1 Department of Public Works

Mandate of the department

The core responsibility of the Department of Public Works is to provide land and accommodation to government departments and institutions. Various information systems are used to maintain and protect the confidentiality, integrity and availability of information, in line with the programmes that form part of the department's annual performance plans, namely Programme 2 (Immovable assets investment management) for lease management and Programme 3 (Expanded Public Works Programme (EPWP) for job creation. This information includes the billing of government departments and payment of landlords.

IT systems used to support and facilitate service delivery were assessed and the following weaknesses were noted

Control weaknesses

Weaknesses identified in the Property Management Information System (PMIS), which supports the process of lease management for creating job opportunities:

- Inconsistencies were noted in the preventative and processing controls developed to ensure that valid and complete lease information would be captured and processed on the PMIS. The risk of fraud and overpayment was further increased by the changes being made to captured lease agreements without supporting evidence to indicate who effected the changes. These inconsistencies can be attributed to ageing technology and the delayed implementation of the iE-Works implementation project that has been in development since 2005 with only 16% of the deliverables completed, despite the project having exceeded its budget by 120%.

The Work-based System (WBS) and the Management Information System (MIS), which are used to report on the beneficiaries of the Expanded Public Works Programme (EPWP), did not have preventative controls to ensure that beneficiaries:

- have valid South African identity numbers
- are not already employed
- are paid the correct wages.

3.4.4.2 Department of Human Settlements

Mandate of the department

The core responsibility of the Department of Human Settlements is to provide housing and give housing assistance to qualifying individuals. The Housing Act, Act No. 107 of 1997, requires the establishment and maintenance of a national housing databank and a national housing information system. In compliance with the act, the Department of Human Settlements uses the Housing Subsidy System (HSS) to manage and administer housing subsidies in line with Programme 3 (Housing development) of the National Housing Code.

IT systems used to support and facilitate service delivery were assessed and the following weaknesses were noted

Control weaknesses

The HSS is a centralised system used to manage housing subsidies.

Control weaknesses within the HSS:

- Management tended to follow manual processes when allocating houses instead of using the system processes that have controls to ensure that houses are allocated to approved beneficiaries.
- The risk of management system overrides was further increased by the lack of standardised business processes across the nine provinces.

Control weaknesses surrounding the HSS:

- Improvements were noted in the centralised provinces (Free State, Gauteng, KwaZulu-Natal, Northern Cape, Limpopo and Mpumalanga), with the exception of the monitoring of user access control, which remained a concern.
- Concerns were noted in the decentralised provinces (Western Cape, North West and Eastern Cape). Specific red flags raised in the Eastern Cape related to user access controls and in the North West included all focus areas audited (i.e. security management, user access controls, IT service continuity). The risks of unauthorised access and data being irrecoverable in the event of a business disruption or IT disaster were exacerbated by the fact that these provinces are responsible for monitoring their own controls, in contrast to the centralised provinces that are monitored by the national department.

3.4.4.3 Department of Health

Mandate of the department

The core responsibility of the Department of Health is to plan, provide and monitor health care services in the country. This includes primary health care services at district level and tertiary health care services at hospital level. Various information systems, such as the District Health Information System (DHIS), are used to collect aggregated anonymous statistical data regarding health facilities from provincial departments, districts and sub-districts in support of the programmes that form part of the department's annual performance plans, namely Programme 2 (District Health Service) and Programme 4 (Provincial hospital services). The data is used to facilitate the planning of health needs in the country.

IT systems used to support and facilitate service delivery were assessed and the following weaknesses were noted

Control weaknesses

Control weaknesses noted within the DHIS:

- Consolidation controls for data received from the provinces were inadequate as manual interventions were possible and no verification processes were in place to ensure the accuracy, validity and completeness of data. Reporting on information such as the number of patients treated, the number of health professionals employed and the number of health care facilities might consequently not be accurate.
- The lack of an integrated data recovery plan for facilities and provinces could, in instances of data corruption or loss, impact on the completeness and availability of consolidated data at the national department. Information on, for example, the number of hospitals to be built or the number of clinics to be provided with water, electricity and sanitation facilities might therefore not be available.

3.4.4.4 Department of Education

Mandate of the department

The core responsibility of the Department of Basic Education is to plan, provide and monitor basic education services in the country. This includes Grade R, primary schools and secondary schools. The department utilises the Education Management Information System (EMIS) to collect aggregated anonymous statistical data regarding the number of learners at education facilities, in line with the programmes that form part of the department's annual performance plans, namely with Programme 4 (Planning Information and Assessment).

IT systems used to support and facilitate service delivery were assessed and the following weaknesses were noted

Control weaknesses

Control weaknesses noted within EMIS:

- Consolidation controls for data received from the provinces were inadequate as manual interventions were possible and no verification processes were in place to ensure the accuracy, validity and completeness of data. Reporting on information such as the number of learners enrolled, educators and non-educator staff employed and the number of learners benefiting from the "no fee school" policy might therefore not be accurate.
- The lack of an integrated data recovery plan for facilities could, in instances of data corruption or loss, impact on the completeness and availability of consolidated learner and school data at the national department. Statistics on, for example, the number of classrooms to be built or the number of schools to be provided with water, electricity and sanitation facilities might therefore not be available.

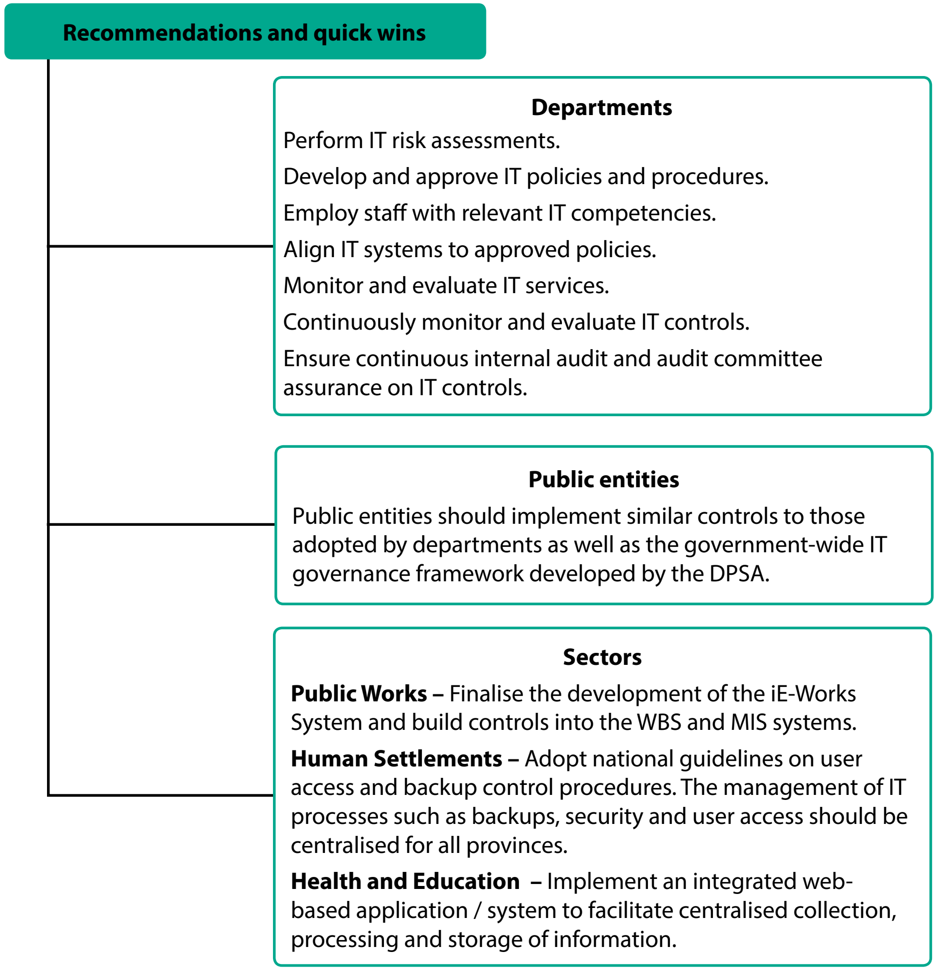
3.4.5 Drivers of IT control weaknesses

- Accounting officers did not view IT as a strategic and service delivery enabler.
- A change in leadership within the DPSA delayed the approval of the government-wide IT governance framework.
- An IT governance framework had not been designed and implemented for public entities and legislatures.
- The lack of consequences for IT control weaknesses contributed to routine tasks, such as the resolution of audit findings and the design and implementation of key controls (policies, procedures, monitoring), not being performed.
- Unfilled vacancies and shortages of key IT skills (IT security officers, network technicians and database administrators) resulted in IT not being properly capacitated to adequately fulfil the required IT control obligations.
- Internal assurance processes, such IT management reporting, internal audit and audit committees, were not effective in supporting leadership oversight of IT.

3.4.6 Recommendations and quick wins in resolving information technology management weaknesses

While we acknowledge that the soon-to-be-implemented government-wide IT governance framework will lay the foundation for medium- to long-term sustainable change in IT across government, we believe that management could proactively address certain issues. For this purpose, we have put together a number of recommendations, some representing quick wins, which would address certain concerns and reduce the impact of current IT exposures.

Figure 33: Recommendations and quick wins



Recommendations and quick wins

Departments

Perform IT risk assessments.

Develop and approve IT policies and procedures.

Employ staff with relevant IT competencies.

Align IT systems to approved policies.

Monitor and evaluate IT services.

Continuously monitor and evaluate IT controls.

Ensure continuous internal audit and audit committee assurance on IT controls.

Public entities

Public entities should implement similar controls to those adopted by departments as well as the government-wide IT governance framework developed by the DPSA.

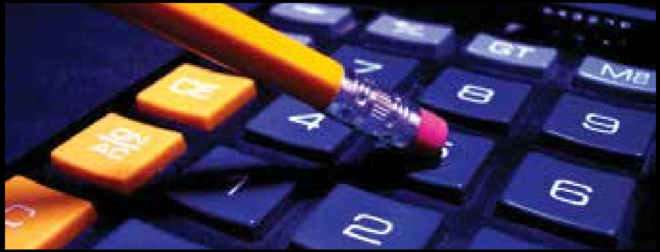
Sectors

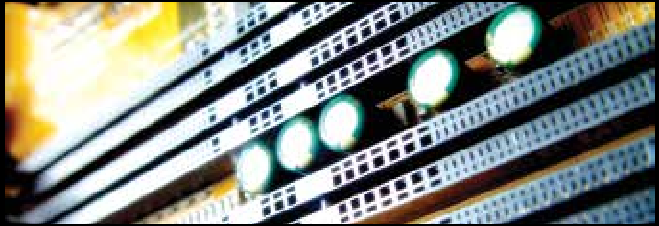
Public Works – Finalise the development of the iE-Works System and build controls into the WBS and MIS systems.

Human Settlements – Adopt national guidelines on user access and backup control procedures. The management of IT processes such as backups, security and user access should be centralised for all provinces.

Health and Education – Implement an integrated web-based application / system to facilitate centralised collection, processing and storage of information.

overview of full report





Visit our website,

www.agsa.co.za,

to view the complete

Consolidated general report on the 2011-12 national and provincial audit outcomes.

RP07/2013

ISBN: 978-0-621-41523-0