12 Information technology controls

12. *Information technology controls*

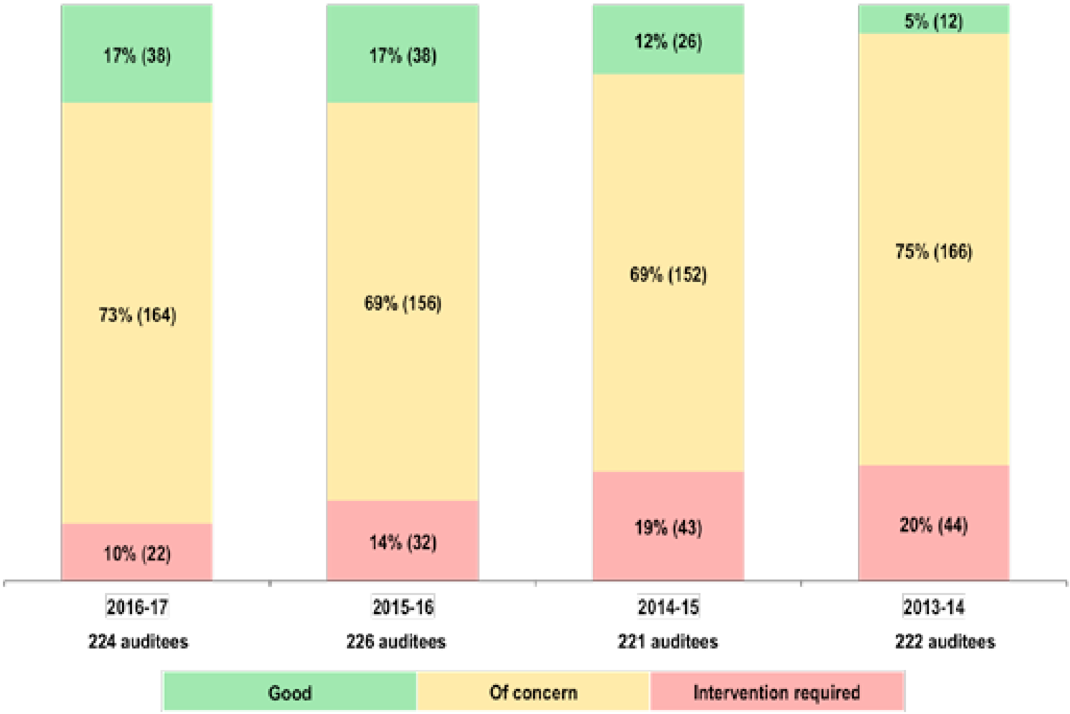
An inherent part of the control environment in national and provincial auditees is the status of their IT controls. **IT controls** ensure the **confidentiality, integrity** and **availability** of state information, enable **service delivery** and promote national **security**. It is thus essential 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 auditee's IT function and ensures that the auditee's IT control environment functions well and enables service delivery. As the majority of financial management controls are automated and monitoring takes place mostly on reports generated by the IT systems, good IT controls and skills are fundamental to enabling robust financial management systems (**DO**) and in-year monitoring (**CHECK**).

Overview of the status of information technology focus areas

Figure 1 shows the status of IT controls since 2013-14.

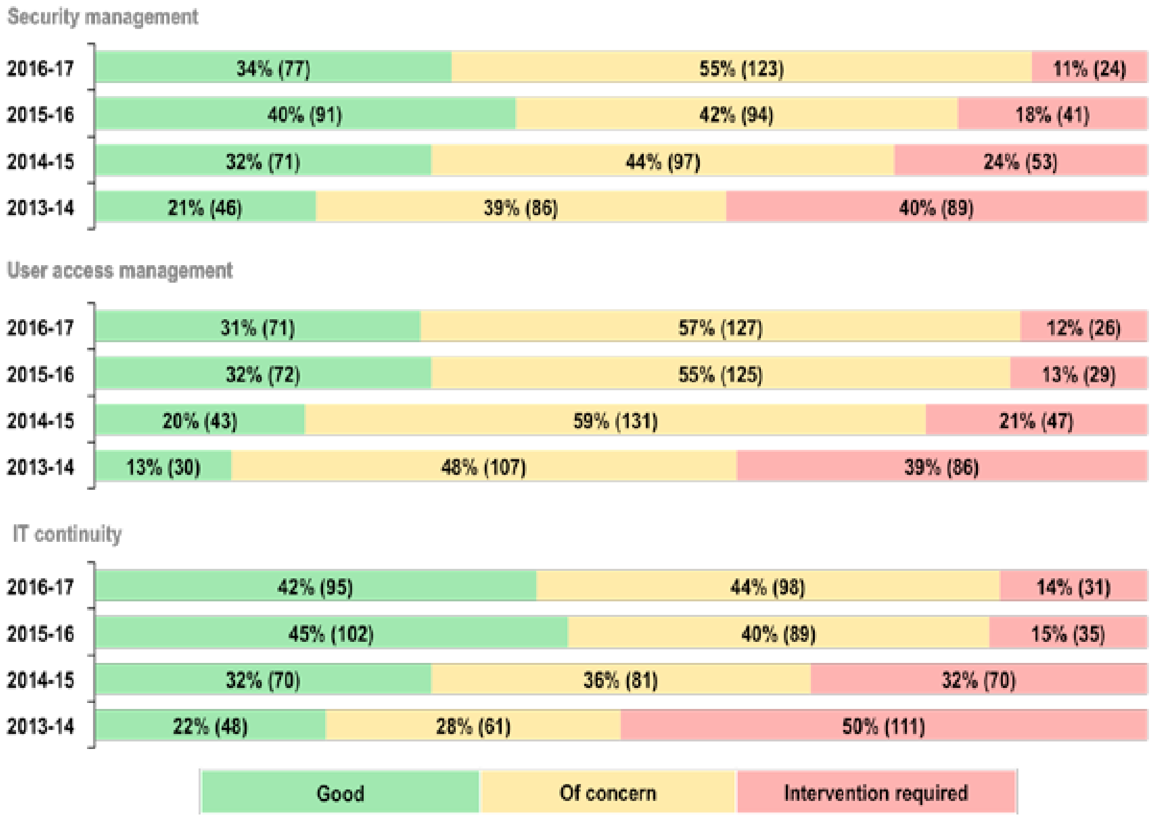
Figure 1: Status of information technology controls



We assessed IT controls at 224 national and provincial auditees with more complex IT environments and found that the number of auditees that had good IT controls increased significantly over the past four years from 5% in 2013-14 to 17% in 2016-17. The improvements were generally due to these auditees becoming more capacitated and taking accountability for their IT environment, but quicker responses are required. We had assessed 226 national and provincial auditees in 2015-16 as opposed to the 224 this year, due to two auditees not signing off on the audit reports as per the deadlines.

Our audits included an assessment of the IT controls in the areas of **security management, user access management** and **IT continuity**. Figure 2 outlines the status of controls in the areas we audited and indicates, per focus area, whether the IT controls were good, concerning or required intervention.

Figure 2: Status of information technology focus areas



There had been an improvement over the past three years in all focus areas and a slight stagnation in the last year, with a significant decrease in the number of national and provincial auditees where intervention was required, indicating that they were moving in the right direction.

Figure 3 further shows an improvement for both departments and public entities from the previous year. The percentage of auditees with a good IT control environment was more or less equal; however, significantly fewer public entities required intervention than departments, due to those charged with governance taking accountability for addressing IT control weaknesses and more staff within the IT sections that were qualified and skilled. However, we remain concerned about the number of public entities at which the IT controls were concerning or required intervention, as the majority of public entities were supported by complex IT environments that were very dependent on adequate IT controls and monitoring by the different assurance providers.

Figure 3: Status of information technology controls – departments and public entities

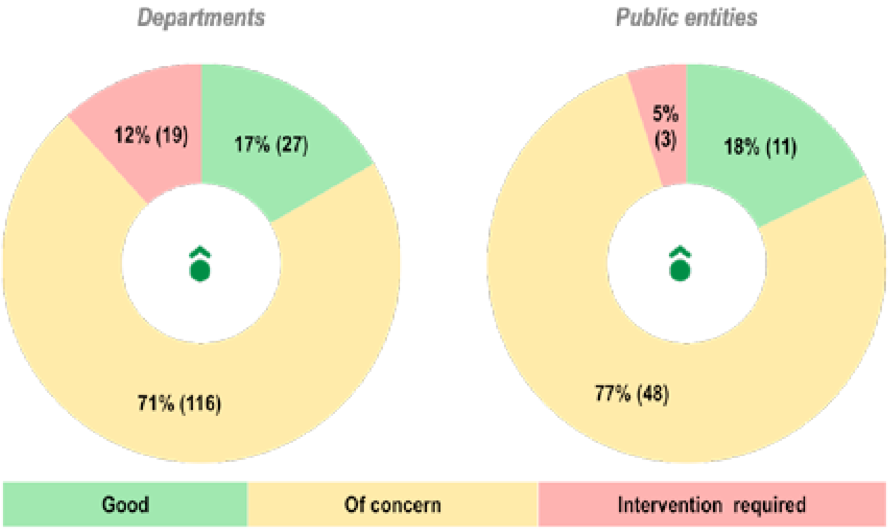


Table 1 indicates the **progress made** since the previous year in addressing areas of concern at national and provincial departments as well as at public entities.

The improvements were generally due to the following:

- More auditees employing chief information officers or IT managers with **adequate qualifications and experience**.
- Auditees **implementing some recommendations** made by the internal and external auditors.
- In Mpumalanga, the **government IT officers** played a **key role** additional to the above-mentioned; and in North West, improvements were mainly due to the **active role** that the **system controllers** played.

Table 1: Progress made in improving information technology controls

Portfolio	Security management	User access management	IT continuity
National departments	↓	↓	↑
Eastern Cape	↓	↑	↑
Free State	↓	↓	↑
Gauteng	↓	↑	↓
KwaZulu-Natal	↓	↓	↓
Limpopo	↑	↓	↑
Mpumalanga	↑	↑	↑
Northern Cape	↓	↓	↑
North West	↑	↑	↑
Western Cape	↑	→	↓
Public entities	↑	→	↓

The **most common findings** were the following:

- Although national and provincial auditees were moving in the right direction and there had been an improvement over the three years overall, the basic IT controls had still not been adequately defined and implemented at most auditees in all three focus areas. Policies and procedures had not been designed or implemented, as also reported in the previous year. Furthermore, the security controls of five provinces and the national departments regressed despite the fact that a number of auditees were still experiencing attacks through their network exposing them to various vulnerabilities, which may have been prevented if security controls had been adequate.
- It is concerning that KwaZulu-Natal regressed in all three areas. This was due to inadequate funding, a shortage of in-house IT skills on lower levels, and systems having functionality limitations.
- A further concern is the regression in two of the three focus areas in the Free State, the Northern Cape, Gauteng and the national departments. This was mainly due to vacancies and a shortage of IT skills on lower levels, budget constraints, and a lack of oversight to ensure that corrective actions were taken and monitored.
- User access weaknesses remained a challenge at the majority of auditees due to a lack of segregation of duties, inadequate reviews of system administrator activities and excessive user access rights. In the case of departments that use transversal systems, the data hosted on these systems is available at the disaster recovery site of the State Information Technology Agency (Sita). However, many departments still did not participate in the Sita transversal disaster recovery testing, as we have reported for the past four years. Where systems are not hosted by Sita, departments and entities have to provide their own data recovery strategies. However, the majority of these auditees still did not have adequate disaster recovery plans and did not test their backups to ensure that they could be restored when required. This could have a major impact on service delivery as the availability of systems is crucial to the achievement of outcomes.
- Public entities continued to increasingly implement enterprise resource planning systems. The enterprise resource planning and project review audits revealed that these systems were not appropriately configured and business requirements were not appropriately documented, resulting in implementations failing or being signed off without understanding the return on investment of these projects. As a result, many of these implementations did not support business objectives and efficiency improvements. Furthermore, there was a lack of sustainability of enterprise resource planning operations, due to excessive reliance on vendors, while system training and the transfer of skills were not prioritised.
- Most auditees did not have automated performance information systems, as also identified in the past four years, but were using Excel spreadsheets to record and report on performance information, which were more susceptible to data manipulation. Adequate performance information systems are key to measuring auditees' service delivery to the public. If information on these systems is not reported accurately and completely, it may have a negative impact on service delivery to the citizens of South Africa.

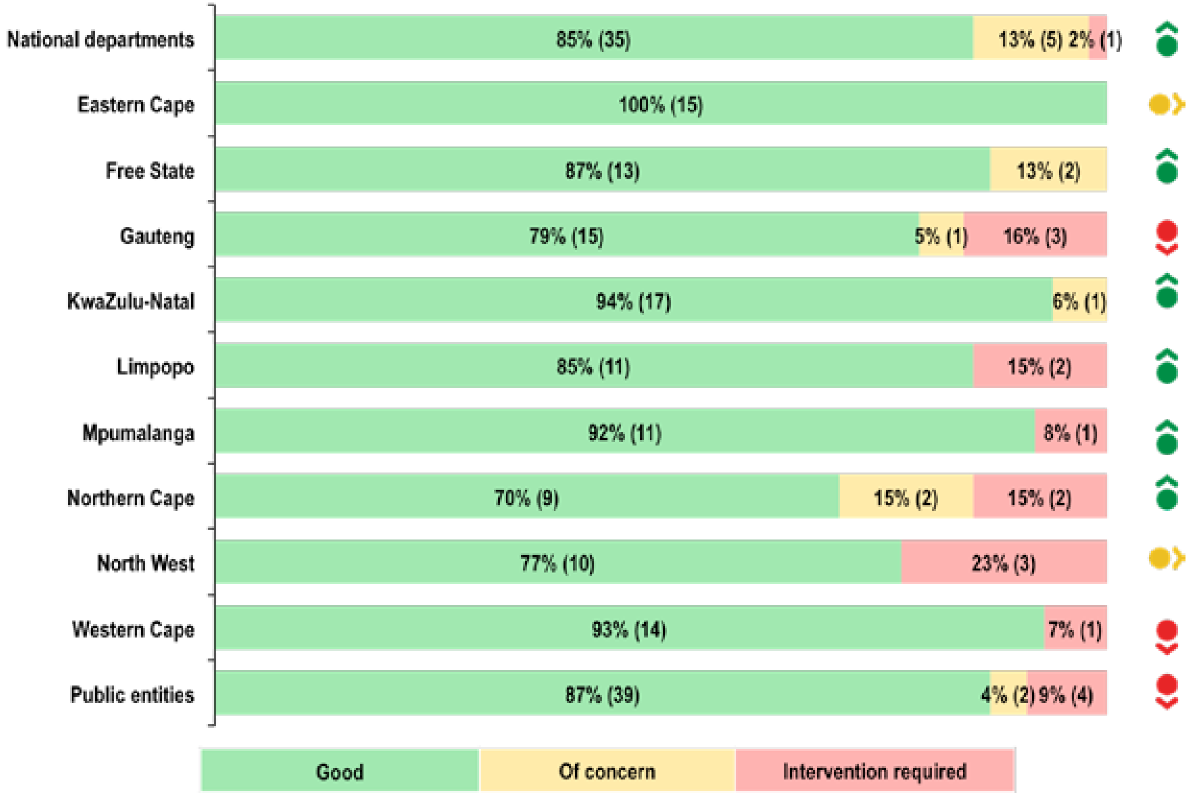
Evaluation of qualifications and experience of chief information officers or information technology managers

Figure 4 indicates that the **qualifications and experience of the chief information officers or IT managers** in government were adequate at most of the auditees, which meant that they had relevant information and communication technology qualifications and six or more years of relevant experience.

Most of the chief information officers or 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. National departments, the Free State, KwaZulu-Natal, Limpopo, Mpumalanga and the Northern Cape improved from the previous year due to more auditees having chief information officers or IT managers with the required level of qualifications and experience as well as vacancies that were filled, while the Eastern Cape was the only province where all auditees assessed had staff with the relevant qualifications and experience. Where national and provincial auditees employed chief information officers or IT managers with adequate qualifications and experience, it had a positive impact on improved IT controls over the past three years.

The regression in Gauteng, the Western Cape and public entities was mainly due to vacancies in positions that had previously been filled or chief information officers and IT managers with inadequate qualifications.

Figure 4: Qualifications and experience – chief information officers or information technology managers

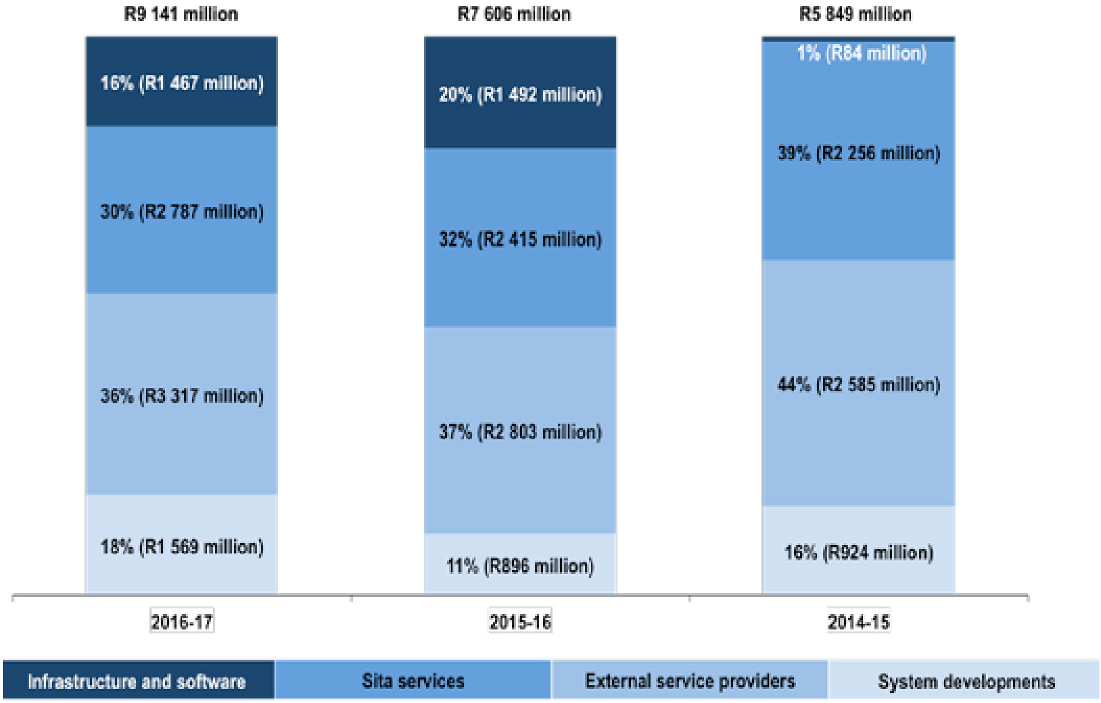


Expenses related to information technology at the provincial and national departments

Figure 5 breaks down the **approximate IT-related expenditure** in terms of **infrastructure and software, Sita services, external service providers** and **system developments**.

IT-related expenditure increased by R3 292 million (56%) in the last two years, with the largest increase in spending being on infrastructure and software as well as system developments, which increased from 1% to 16% and from 16% to 18% of the IT-related expenditure, respectively. This was due to revitalisation and modernisation projects undertaken by some of the key departments and provincial departments to enhance broadband, upgrade internet links, replace ageing servers and install next-generation firewalls. The increase was evident in all the provinces and at national government level. The amounts spent on Sita support services and services rendered by external service providers were more or less equal. Expenditure in this regard did not significantly increase from the previous year but overall represented 66% of the total amount spent – representing the largest part of the IT expenditure. Despite this, we found that the performance monitoring processes of service providers were inadequate. This resulted in payments being made by departments without monitoring whether services were delivered at the agreed upon level of quality, due to the lack of, or inadequate, project management offices within government, as we had also reported previously.

Figure 5: Expenses relating to information technology at national and provincial departments



Large information technology projects currently underway

Integrated financial management system project

The IFMS project, managed by the National Treasury, awarded the contract to replace the ageing transversal financial systems (BAS, Persal and Logis) to Oracle as the only software solution provider in April 2016. Although a project management office was established as reported last year, the contract had been suspended and the responsibilities moved to internal staff of the National Treasury, which now have to come up with a new plan on how this function will be managed. The project governance framework has been formalised and is being implemented. With the appointment of the solution provider, the project aims to implement the revised IFMS solution by 2022, as previously reported.

The roles and responsibilities as reported last year in providing independent assurance were still being formalised between ourselves, the National Treasury, Department of Public Service and Administration (DPSA) and Sita, as the DPSA requires additional clarity on their involvement on the IFMS project before signing off on the IFMS audit strategy and framework. To ensure proper oversight of the project, the National Treasury's internal audit function continues to audit the IFMS project from time to time to highlight possible risks and concerns to management.

We are also focusing on the IFMS programme's contracts and SCM processes through our normal regularity audits at all affected auditees, and reported on this in their reports during the 2016-17 financial period. Concerns included a lack of an approved and detailed project plan indicating milestones by when tasks must be completed and signed off by service providers. Therefore, accountability and consequence management would have been difficult to enforce (**ACT**). There was also no detailed budget per year for the IFMS project, which made it difficult to track and report on the actual expenses relating only to the IFMS – the actual amount spent as at 31 March 2017 could thus not be determined.

Integrated justice system (IJS)

The objective of the IJS programme is to electronically enable and integrate the end-to-end criminal justice business processes. Once fully operational, the IJS will enhance the efficiency and effectiveness of the entire criminal justice process by increasing the probability of the successful investigation, prosecution and punishment for priority crimes and, ultimately, the rehabilitation of offenders.

The IJS programme management office had made great strides in addressing project governance issues identified during the 2015-16 review, but project artefacts were still not in place. Additional issues identified during the 2016-17 review included the inadequate use of prescribed templates and a failure to update project information on the Project Portfolio Office system; the lack of an organisational change readiness report; the absence of key project management artefacts; and the lack of training, organisational change management, and operational support plans. An assessment of the IJS modernisation programme revealed a lack of progress on some of the key project deliverables scheduled for 2016-17, resulting in the shifting of deliverables to the next financial year. Although approved, shifting these timelines will have a negative impact on the overall delivery of the IJS.

Approximately R4,67 billion had been spent on the IJS programme as at 31 March 2016, over a period of more or less 12 years since 2004, against a budget of R4,92 billion as reported by the IJS project management office. In comparison, as at the end of the 2016-17 financial year, spending on the IJS programme was under R5 billion, against a budget of R5,26 billion. The budget spent during the 2016-17 financial year related to progress made in implementing and upgrading IJS-related information systems (such as the electronic case management system, inmate integrated management system, electronic court filing system, and integrated case management system), and infrastructure development and upgrades by the eight IJS member departments.

e-Government, e-Health and e-Education strategies

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 information and communication technology. To ensure the successful implementation and effective monitoring by the DPSA of this strategy, the Public Service Regulations of 2016 require that the minimum norms and standards for information and communication technology be developed and monitored by the DPSA.

Therefore, Sita revised the Minimum Interoperability Standards and submitted these to the DPSA. The standards are currently being reviewed by the DPSA's legal services and have not yet been finalised. As the Minimum Information Security Standards remain a contested area, they have been taken out of the revised Public Service Regulations of 2016, as they are believed to fall under the minister of Security. No discussions relating to updating this document took place during the period under review.

The position of government chief information officer in the DPSA had not been filled for more than six years, with acting incumbents dating back to 2011. The lack of stability in this role has had an impact on the timely finalisation and implementation of standards, guides and procedures to be issued to departments. In addition, this had an impact on the improvement of the IT control environment within government, as most departments were still struggling with the implementation of the Corporate Governance Information and Communication Technology Policy Framework.

e-Health

The e-Health Strategy South Africa 2012-16 is aimed at reducing waiting times, improving data quality and integrity, increasing timely access to data, streamlining registers, and strengthening information management in the public health sector.

Little progress had been made with the implementation of this strategy in the provinces, due to budget constraints, IT-critical vacancies and a lack of prioritising the implementation of the initiatives. Provincial health departments had also not been monitoring the e-Health initiatives. In addition, minimal progress had been made regarding the development of information and communication technology infrastructure, network connectivity as well as the integration of systems, with the exception of Gauteng that recently embarked on an information and communication technology infrastructure upgrade.

Two provinces (Limpopo and North West) had still not developed their e-Health strategies, as reported previously, due to senior management not taking accountability to prioritise this initiative. Furthermore, the eHealth strategy was still in draft format in the Eastern Cape as it was only prioritised during 2016-17, while only the Northern Cape had incorporated e-Health initiatives into their approved IT strategy.

All provinces still faced challenges relating to connectivity and interfacing key systems (such as billing, patient registration and pharmaceutical systems), which contributed to the objectives of the e-Health Strategy South Africa 2012-16 not being achieved yet.

e-Education

The White Paper on e-Education (2004) revolves around the use of information and communication technology to accelerate the achievement of national education goals. The main outcome is to increase access to such technology to support curriculum delivery and improve learner attainment.

The Department of Basic Education has continuously been monitoring the measures put 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 information and communication technology development for management, teaching and learning; and access to information and communication technology infrastructure and connectivity.

In previous years, four provinces had delayed the implementation of this white paper due to challenges around the availability of budgets at provincial level, inadequate broadband infrastructure especially in rural areas, and teachers' limited capability to use information and communication technology.
However, during the 2016-17 financial period, Limpopo developed a strategy that was aligned to the white paper that drives the initiatives of e-Education. Two provinces (Eastern Cape and North West) had started with the development of e-Education strategies, which still had to be approved. Only the Northern Cape had not started developing e-Education strategies, as resources have not yet been allocated to this initiative.

In addition, due to the slow movement and lack of skills in some provinces, the department rolled out the operation phakisa initiatives as an implementation plan to all the provinces and different role players to assist in the information and communication technology education rollout plan.

Inadequate progress and a lack of monitoring and prioritisation by senior management in the provinces could result in the e-Education strategy not being implemented, thus ultimately hampering the achievement of quality education in the country.

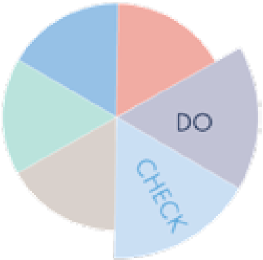
Most common root causes

Most of the common root causes remained the same as in the past four years, demonstrating a lack of accountability by those who had to ensure that decisions and actions were implemented and that consequence management was enforced. The most common root causes remained the following:

- Although the **skills and experience** in departments and public entities were adequate at **chief information officer or IT manager level,** with only 5% of these positions being vacant at year-end, auditees could not attract staff to fill vacant key positions such as those of system controllers and information security officers. Furthermore, some IT divisions did not operate on a strategic level to influence the design and implementation of adequate policies and procedures.

- The **chief information officers, IT managers and IT staff** did not fulfil their **responsibilities** by ensuring compliance with the controls established to secure and regulate their departments' IT environments, due to a lack of consequence management.
- The **accounting officers and accounting authorities** did not prioritise the **approval of IT policies and procedures** to ensure that proper internal controls existed and could be enforced.
- The **performance monitoring processes of IT service providers** were not adequately enforced to ensure that services were rendered at the agreed level of quality or standard.
- Most departments were fixing **symptoms** rather than implementing improved IT controls. Another major concern was the ineffectiveness of **those charged with governance**, as they were not proactive in addressing the audit findings and preventing recurrences.
- The replacement of outdated infrastructure and software to improve IT controls was hindered by **insufficient funding**. Although there was a significant increase in spending over the last two years due to a few key departments that were modernising, it may take a few years to address the backlog of outdated infrastructure and software that currently exists in government.

Conclusion



As the majority of financial management controls are automated and monitoring takes place mostly on reports generated by the IT systems, good IT controls and skills are fundamental to enabling robust financial management systems (**DO**) and in-year monitoring (**CHECK**).