# 7 Information technology controls

## 7. Information technology controls

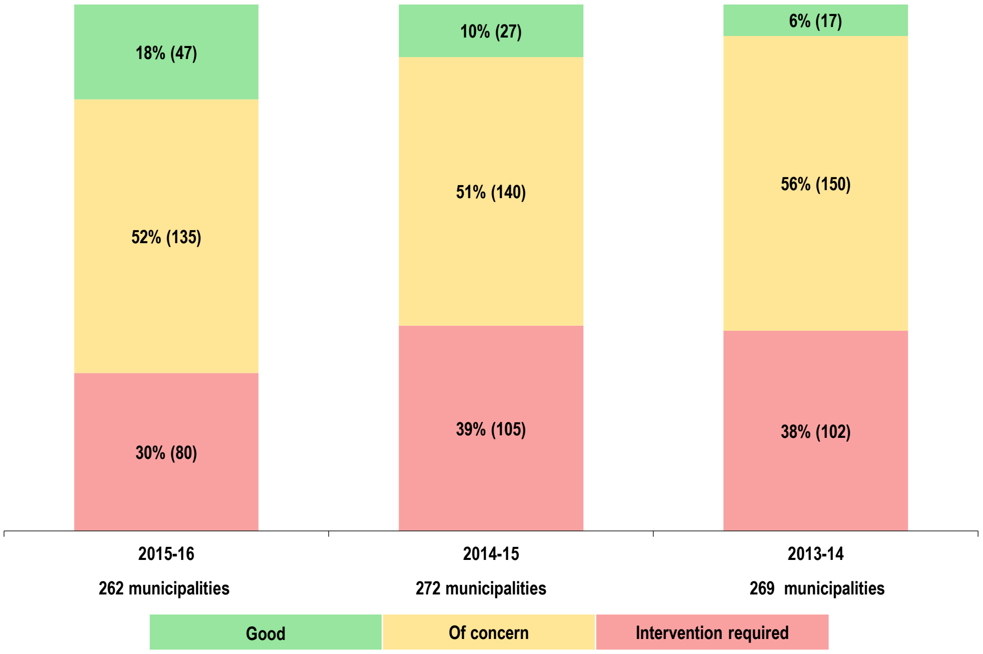
**An inherent part of the control environment in municipalities is the status of their IT controls. IT controls** ensure the **confidentiality, integrity and availability** of state information, enable **service delivery** and promote **security** in local government. It is thus essential for good IT governance, effective IT management and a secure IT infrastructure to be in place.

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

## Overview of the status of information technology focus areas

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

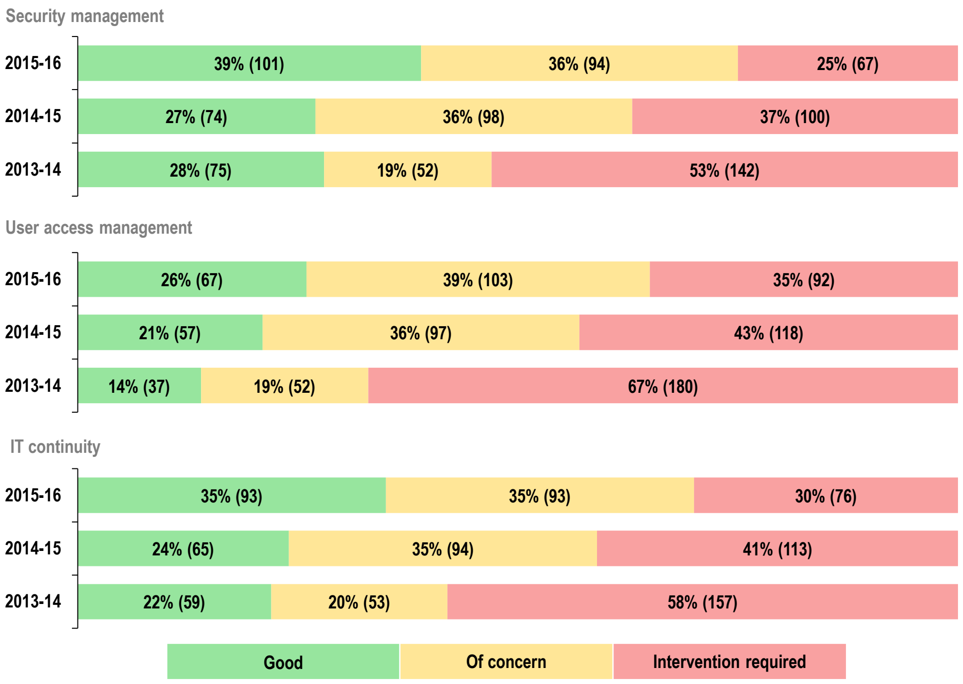
Figure 1: Status of information technology controls



We assessed IT controls at 262 municipalities and found that the number of municipalities that had good IT controls in place increased significantly from 10% in 2014-15 to 18% in 2015-16. The improvements were generally due to the capacitating of, and increase in support to, municipalities by coordinating departments. We had assessed 272 municipalities in 2014-15.

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

### Figure 2: Information technology focus areas



There had been an improvement over the two years in all focus areas, with a significant decrease in the number of municipalities where intervention was required, indicating that municipalities were moving in the right direction.

Table 1 indicates the **progress made** since the previous year in addressing areas of concern at municipalities. The improvements were generally due to the following:

- **Coordinating departments** were playing a pivotal role in capacitating and supporting municipalities.
- More municipalities were employing CIOs or IT managers with **adequate qualifications and experience**.
- Municipalities **implemented some of the recommendations** made by internal and external auditors.

### Table 1: Progress made in improving information technology controls

| Province | Security management | User access management | IT continuity |
|---|---|---|---|
| Eastern Cape | ↑ | ↑ | ↑ |
| Free State | ↑ | ↑ | ↑ |
| Gauteng | ↑ | ↓ | ↑ |
| KwaZulu-Natal | ↑ | ↑ | ↑ |
| Limpopo | ↑ | ↓ | → |
| Mpumalanga | ↑ | ↓ | ↑ |
| Northern Cape | ↑ | ↓ | ↑ |
| North West | → | ↑ | ↑ |
| Western Cape | ↑ | ↑ | ↑ |

The most common findings were the following:

- Most of the metros remained concerning or required intervention, while the City of Johannesburg Metro and Ekurhuleni Metro regressed from the previous year. This was due to some metros still experiencing challenges to fill vacancies in key positions, such as those of the CIO and specific positions within the IT section. Furthermore, some metros were still experiencing weaknesses in internal control. This included not establishing an IT governance framework, isolated security vulnerabilities, IT steering committees being inactive, action plans not being implemented and monitored, and disaster recovery plans not being tested to ensure the recovery of data in the event of a disaster.
- Although municipalities were moving in the right direction and there had been an improvement over the two years in all areas, a number of municipalities still had not adequately defined and implemented basic IT controls in the security management, user access management and IT service continuity areas. The regression in user account management in Limpopo, Mpumalanga and the Northern Cape was mainly due to inadequate management oversight to ensure that prior year commitments had been implemented. Policies and procedures were not designed or implemented, as also reported in the previous year. Some municipalities experienced security breaches as security controls were compromised, resulting in fraudulent activities. Some municipalities were still highly dependent on IT service providers and in many instances their performance was not monitored to ensure the agreed-upon level of quality was delivered. System administrator activities and user access rights were not always reviewed and the segregation of duties was not in all instances maintained. Furthermore, the management of backups remained a challenge, as most of the municipalities did not test their backups to ensure that they could be restored when required.

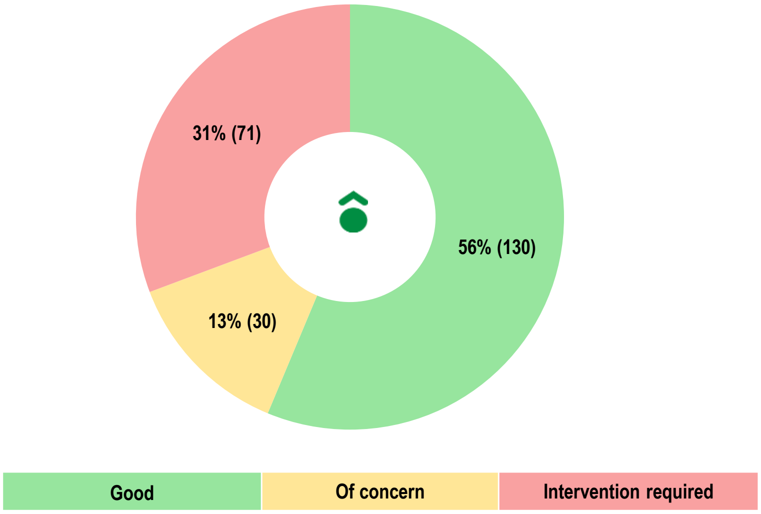
The challenges experienced with regard to adequate security management, user access management and IT service continuity were made worse by the following factors:

- Municipalities experienced budget constraints, which limited the development of IT policies and procedures. In other instances, already developed IT policies and procedures were still awaiting approval from management and the council.
- Service level agreements with vendors did not include the management or development of IT policies and procedures.
- District municipalities did not provide adequate guidance and support to the local municipalities under their jurisdiction.
- Staff did not fulfil their responsibilities in terms of ensuring compliance with the controls established to secure and regulate municipalities' IT environments. Moreover, they were not held accountable for failing to address previously raised findings.

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

Figure 3 indicates that, for most of the municipalities, the **qualifications and experience of CIOs or IT managers** in local government had improved from the previous year and were adequate, which meant that they had relevant information and communication technology qualifications and six or more years of relevant experience.

Figure 3: Qualifications and experience – chief information officers or information technology managers



Overall, 56% of municipalities employed CIOs or IT managers with the necessary qualifications and experience to implement the IT governance structures and controls and to ensure an improvement in IT controls. Where municipalities employed CIOs or IT managers with adequate qualifications and experience, it had a positive impact on the improvements over the two years.

The municipalities where intervention was required in many instances had **failed to fill the position**. However, some municipalities still **did not have an approved position** for this function on the organisational structure. In such instances, municipalities made use of consultants to ensure that IT roles and responsibilities were fulfilled; however, the performance of consultants was not monitored closely. Furthermore, it was a concern that although these positions had been filled at some municipalities, the CIO or IT manager did not have the appropriate qualification and/or years' experience required for the position. The above may have contributed to the areas of concern and where intervention was required with regard to IT controls.

## *Information technology support provided by coordinating departments*

Coordinating departments play a pivotal role in **capacitating and supporting municipalities**, especially in respect of the implementation of mSCOA. The roles of each coordinating department are interlinked, but with a clear indication of the support to be provided.

Table 2 indicates whether these coordinating departments provided support to municipalities.

**Table 2: Support provided to municipalities by coordinating departments**

| Province | Provincial Cogta | Provincial treasury | Office of the premier |
|---|---|---|---|
| Eastern Cape | No | Yes | No |
| Free State | Yes | Yes | Yes |
| Gauteng | No | No | No |
| KwaZulu-Natal | Yes | Yes | No |
| Limpopo | Yes | No | Yes |
| Mpumalanga | Yes | Yes | Yes |
| Northern Cape | Yes | No | Yes |
| North West | Yes | No | Yes |
| Western Cape | Yes | Yes | Yes |

The **DCoG** established an information and communication technology think tank made up of officials from the National Treasury, departments of cooperative governance, the State Information Technology Agency, the Department of Public Service and Administration and our office (as an observer), as previously reported. However, the structure did not function during the latter part of 2015-16. Provincial Cogtas supported their municipalities in at least seven of the nine provinces as indicated in table 2, but in some provinces they did not have adequate capacity to effectively support all municipalities.

The **offices of the premier** continued to invite municipalities to attend **meetings of the provincial government IT officers** and are rolling out processes that will provide assistance to municipalities that are struggling with the implementation of IT controls.

The **National Treasury** issued guidance through MFMA SCOA circulars and rolled out accredited training initiatives on mSCOA implementation. Provincial treasuries are responsible for providing budgetary assistance to municipalities and for facilitating arrangements for non-accredited mSCOA training sessions.

We recommend that the coordinating departments that have not supported municipalities as indicated in table 2, take the following actions:

- Provincial Cogtas should strengthen their capacity to effectively support the municipalities in all provinces.
- All coordinating departments should share their supporting strategies across provinces so that they can leverage on each other's success.

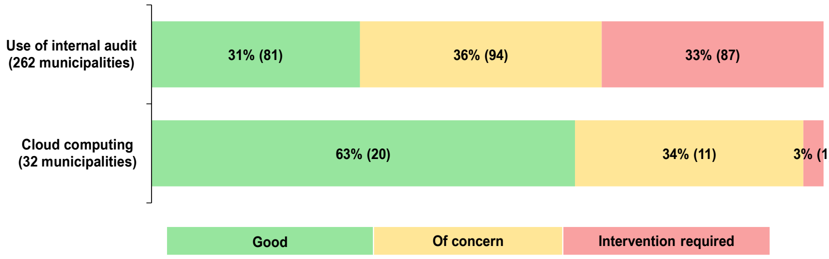
## Information technology health within local government

Municipalities should (i) perform their operations in a secure IT environment, (ii) operate effective financial systems to enable the presentation of credible information on a timely basis for internal and external use, and (iii) enable their internal audit functions to provide the level of assurance required by those charged with governance.

We therefore assessed IT health within local government at municipalities by focusing on the IT audit skills within internal audit units as well as cloud computing.

Figure 4 indicates the results of these assessments.

### Figure 4: Information technology health within local government

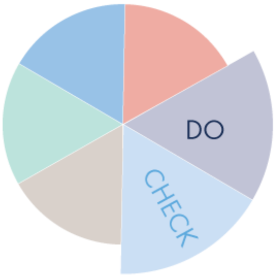


We assessed the **internal audit units** of municipalities and found that 31% of these municipalities had an internal audit function that performed IT audits, while 36% of them were assessed as concerning as they had the capacity to perform IT audits, but were not yet performing this function. Most municipalities therefore had sufficient capacity in their internal audit function to evaluate their internal controls in the IT environment, perform risk management, and evaluate governance processes to provide the assurance required by management.

**Cloud computing** and storage solutions are an emerging technology that provides municipalities with various capabilities to store and process their data in third-party data centres that may be located far from the municipality or even outside the country. We found during our assessment that most municipalities were not yet utilising cloud computing, with only 32 indicating that they were making use of these services. From these few municipalities, we further found that 63% of them had adequate internal controls to manage this environment, while the remaining municipalities were concerning or required intervention. The latter is of concern, as the following are some of the business risks associated with cloud computing:

- Sharing resources increases the risk of private information leaking to others in the cloud.
- The unavailability of data and services may have an impact on the business of the municipality.
- Security may be breached with shared access control, while the risk of unprotected data may increase.
- Cloud providers may become the owners of the data, as this could be included as a clause in the agreements between cloud providers and municipalities.

We also assessed the readiness of municipalities to use the **central supplier database** and to start inviting bids through the **eTender portal**. Refer to section 4.2.1 on the readiness for SCM reforms for more detail on the results of the assessment.



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**).

## NOTES