IMPROVEMENTS IN IT CONTROLS NEEDED FOR LOCAL GOVERNMENT: 2013 AGSA REPORT

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | July 31, 2014

The Auditor-General of South Africa ("**the AG**") recently released his 2012-2013 consolidated general report on the audit outcomes of local government, 30 July 2014 ("**the report**").

The report addresses six risk areas, one of which is Information Technology ("**IT**") controls. The fact that IT is one of the six risk areas audited by the AG, highlights its importance in the proper functioning of local government and municipal owned entities.

The AG assessed IT controls using five criteria. These were: security management; user access management, IT service continuity, formal control over IT systems and IT governance.

Security management: As far as security management is concerned, the AG found that: "*while 28% of the auditees had IT controls that were embedded and functioning effectively, 60% of the auditees continued to experience challenges with design and 12% experienced challenges with the implementation of security management policies.*" One of the most common findings was that IT security parameters were not being "*effectively configured to protect the IT infrastructure from unauthorised access.*"

User access management: User access policies also proved challenging. 68% of those audited continued to experience challenges with the design of user access policies. 16% fared slightly better as they seem to have had policies, but their issues related to the actual implementation of the user access policies.

IT service continuity: The outcomes in this area are worrisome. 30% of those audited had IT controls that were embedded and functioning properly. 62% experienced challenges with design and 8% experienced challenges with the implementation of adequate IT service continuity controls. A finding that needs urgent attention, particularly if e-government is being punted as a solution to inefficiency, is that most municipalities do not test their back-ups and back-ups are not stored off-site.

Formal control over IT systems: The AG identified a lack of skills as a major root cause of challenges in IT controls. The AG recommends the reallocation of funds to upskill IT staff; the enforcement of consequences for repeat adverse IT findings; the transfer of skills from service providers; and internal audit units and audit committees needing to play a more effective role.

IT governance: The AG highlights the fact that the Corporate Governance of Information and Communication Technology Policy Framework ("the **ICT Framework**") has been developed by government and approved by cabinet. It has however not been implemented. The AG points out that all those who were audited are required to adopt and implement the ICT Framework over the next three financial years i.e. 2014 onwards. It is clear from the AG's report that it is expected that the Department of Cooperative Governance and Traditional Affairs ("**CoGTA**") will have a crucial role to play in the implementation of the ICT Framework.

Given the regular and very public data breaches and theft of sensitive information that are reported on a daily basis, the issues that the AG points out need to be addressed as a matter of urgency. IT audits or gap analyses need to be conducted, their findings need to be implemented, skilled staff need to be recruited or existing staff need to be upskilled and IT governance must be implemented from the top down. These are important priorities that must be pursued immediately.

If South Africa is to really grow and implement e-government, e-health and e-education effectively, as is envisaged in *South Africa Connect: the National Broadband Policy 2013* and *SIP 15: Expanding access to communication technology*, the AG's 2014 and 2015 findings on IT controls need to be looking vastly different to his current report.