RE ŠOMA LE SETŠHABA

CAPRICORN DISTRICT MUNICIPALITY

CRITICAL ICT FINDINGS RAISED BY THE AGSA and how they can be addressed

Presented by:

Ms. Hellen Mamabolo, CDPSE, (Mphil: IT Governance)

Senior IT Audit and Risk Specialist

14 July 2022

KODUMELA
BLOUBERG MUNICIPALITY

MOTHO KE MOTHO KA BATHO

Molemole Municipality

CITY OF Polokwane
NATURALLY PROGRESSIVE

AGENDA

1. Introduction
2. Overview
3. Background
4. ICT Findings as per the <u>Component</u>
   - IT Governance
   - Security Management
   - User Account Control
   - Program Change Management
   - Facilities & Environmental Controls
   - IT Service Continuity

5. Conclusion

ICT AUDIT

Is an examination and evaluation of the municipality’s IT infrastructure, policies and operations

- It determine whether IT controls
  - ✓ Protect municipal assets to ensure data integrity
  - ✓ Are aligned with the municipality’s goals and objectives

OVERVIEW

This presentation provides an overview of the critical Information and Communication Technology findings that are raised by the Office of the Auditor-General to the municipalities

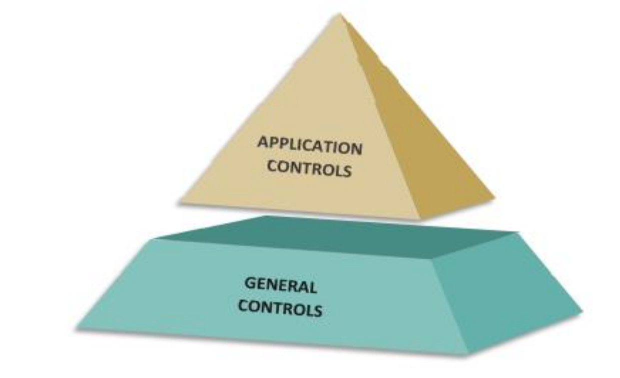
BACKGROUND

IT CONTROLS are classified into two types:

IT General Controls

Are broad in scope and relates to the environment in which applications are maintained and operated; therefore, general controls affect all applications.

We cannot rely on IT systems or data therein **without effective IT General Controls**

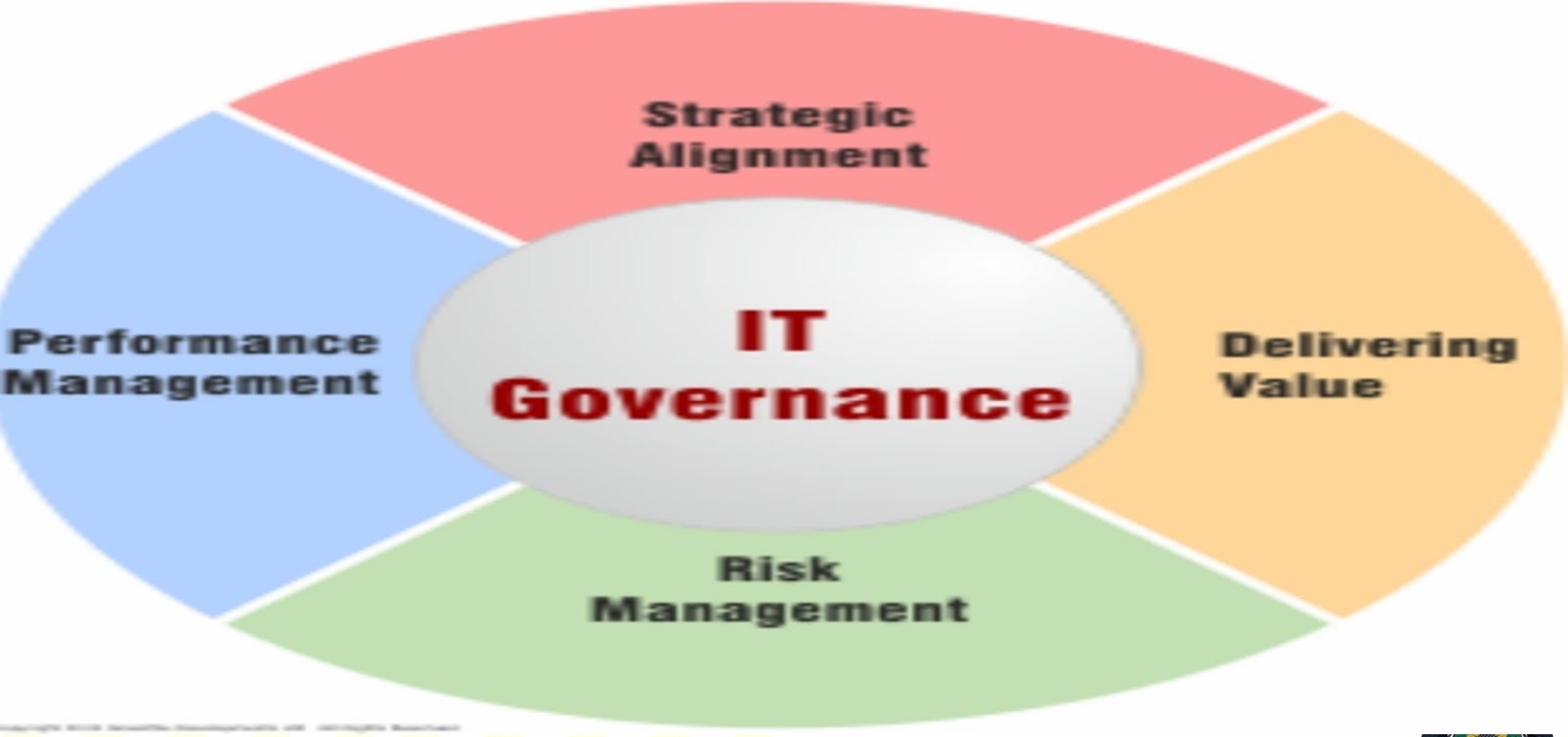


IT Application Controls

Are narrow in scope; usually specific to an individual application; and are designed to ensure that only complete, accurate, and valid data is entered into and processed by an IT application.

IT GOVERNANCE

According to **Principle 12 of King IV**, the purpose of IT Governance is to support the organisation to set and achieve its objectives.



IT GOVERNANCE

Finding 1: IT Strategic Plan

The document should be updated to ensure that ICT service delivery are aligned with the strategic goals of the municipality.

IT GOVERNANCE

Finding 2: Inadequate reporting on service provider performance of Service Level Agreements (SLAs).

- SLA is considered as an important part of the IT Governance framework and of the end-user support structure.
- Not only must it be established but it must also be strictly monitored and adhered to if the service support structure is to succeed.
- ICT service performance must be assessed on an on-going basis to identify gaps between what was expected and what was realised.

IT GOVERNANCE

Finding 3: Inadequate conduct of skills gap or needs analysis.

- Municipalities rely on information technology to **help them be more productive**.
- IT officials need to attend trainings to maintain continuing education programmes for professional certifications (where applicable) and to be **kept abreast** of the latest developments in technology.
- Auditors should be well equipped in order to provide assurance to management and stakeholders

IT GOVERNANCE

Finding 4: Inadequate IT Staff Resourcing

Key IT positions should be filled to enable the IT department to fulfil its role effectively by adequately supporting the municipality's business units.

SECURITY MANAGEMENT

Finding 1: Inadequate firewall rules settings

- Firewall rules should be adequately set and the firewall keeps logs to allow management to review any changes or activities performed by the firewall administrator on a regular basis.
- Firewall rules should be updated accordingly or when changes occurred in order to prevent hackers from gaining access to the municipal network.

SECURITY MANAGEMENT

Finding 2: Inadequate antivirus management

- Failure to ensure that the network servers have the latest anti-virus, service packs and security patches applied increases the risk that unauthorised activity may occur and that known Windows security vulnerabilities may be exploited.
- Antivirus definitions should be automatically updated when the computer user connects to the municipal network in order to provide reactive protection against breaking threats before they can widespread.

USER ACCESS CONTROL

Finding 1: **The user access functions/profiles for the financial system (e.g. Phoenix, Solar) and payroll (e.g. Payday) system were not reviewed.**

- Management should review users’ access rights at a regular interval using formal processes after any changes such as promotion, demotion, or termination of employment.
- User access rights should be reviewed and re-allocated when moving from one employment to another within the same organization.
- Authorizations for special privileged access rights should be reviewed at more frequent intervals.

USER ACCESS CONTROL

Finding 2: Non-compliance with password policy

Strong password requirements, such as minimum length, expiration after a defined number of days, and complexity, establish the validity of a user’s claimed identity and helps safeguard critical IT resources.

USER ACCESS CONTROL

Finding 3: Lack of adequate segregation of duties

User access should be assigned so that no one individual controls all critical stages of a process or transaction.

e.g. No user should be able to perform all stages within the expenditure process: enter/approve the purchase order, post the receipt, post the vendor invoice, and perform the cash disbursement.

CHANGE MANAGEMENT

Finding 1: No formal change management process

Municipalities need to develop, document, and/or implement a change management process to ensure that system changes consistently comply with their policy.

- Changes should be approved and authorised
- Changes should be tested
- Changes should be documented and tracked (change management logs)

Inadequate change management processes can affect system and service availability, such as unplanned system down-time.

FACILITIES & ENVIRONMENTAL CONTROL

Finding 1: Unauthorised access to the server room

The server room should be physically secured during and after business hours.

The following should be in place:

- Bolting door locks
- Manual logging
- Biometric
- Identification badges
- CCTV
- Security guards
- Deadman doors
- Controlled single entry point
- Alarm system

FACILITIES & ENVIRONMENTAL CONTROL

Finding 1 continue:

- Access to the server room should be restricted to authorized persons only; authentication controls, e.g. access control card plus PIN.
- Third party support service personnel should be granted restricted access to the server room only when required.
- This access should be authorized and monitored, therefore the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised.

"An audit trail of all access should be securely maintained"

FACILITIES & ENVIRONMENTAL CONTROL

Finding 2: Inadequate maintenance of the supporting utilities

- Support utilities (e.g. UPS, Backup generators, fire suppression systems, fire extinguishers, air conditioners, etc.) must be regularly inspected and maintained in accordance with the supplier’s recommended service intervals and specifications
- They should also be tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

IT CONTINUITY

Finding 1: Inadequate design and implementation of the Disaster Recovery Plan (DRP)

- BCP should be developed and approved which should include the recovery strategy with all of its detailed components and the test plan
- Implement the plans to minimize the impact on the municipality and recover from the loss of information assets to an acceptable.
- Management should perform BIA to identify the activities that are key to survival, also known as critical business activities within the municipality.
- BCP/DRP should also be tested regularly to verify the effectiveness of the plan and to ensure that it can be reliably implemented in an emergency situation.
- Employees should be trained and tested on the performance of emergency management, business continuity, and disaster recovery operations.
- Disaster Recovery Site should be in place.

IT CONTINUITY

Finding 2: Inadequate backup testing and restoration

- Backup media should be regularly tested to ensure that they can be relied upon for emergency use when necessary.
- Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Why there is need to address the Audit Findings?

Failure to address the audit findings may result in business operations disruptions and delay the issuance of the audited financial statements.

THANK YOU

Re šoma le setšhaba

Hellen Mamabolo, CDPSE I Senior IT Audit & Risk Specialist

☎ 015 294 1018 📱076 752 9125 📠 086 628 0207

Email: mamaboloh@cdm.org.za

CAPRICORN
DISTRICT
Municipality