Information Technology (IT) Audit; Risk and AOPO Workshop – ITGCs; ITACs & Project Assurance

CIGFARO

July 2019

Presented by

Sithabile Zungu (Sithabile.Zungu@sng.gt.com; 0762003243)

Contents

ITGCs and ITACs

ITGCs – controls that exist within the IT environment before transactions are processed:

- Access controls
- Security controls
- Program change controls
- Backup and restore controls
- Disaster recovery
- Incident and change management
- IT governance

ITACS – business process or application system:

- Data edits
- Separation of business functions
- Balancing of processing totals
- Transaction logging
- Error reporting

AGSA Audit Outcomes 2017/18 – ITGCs

Disaster Recovery Plans	• Not in place • Not approved { 9 Municipalities (+/-30%) }
Administrator / Controller Access	• Lack of monitoring • Lack of review { 8 Municipalities (+/-30%) }
IT Security Policies & Procedures	• Not in place • Not approved
Security Settings	• Inadequate security settings not in accordance with best practices { 11 Municipalities (+/- 40%) }
Reliance on IT vendors	• Support of application systems

AGSA Audit Outcome - Impact of ITGCs control weaknesses

- The 2017/18 AGSA summary report points out that “weaknesses identified in ITGCs had a direct impact on the credibility of information produced by these systems and subsequently the information submitted for auditing meaning the governance at the municipalities is compromised”

- In other words IT controls that would detect and prevent the risk of fraud and error were not effective

AGSA Audit Outcome - The Role of Internal Audit

Internal Audit Activity (IAA) plays a key role in providing independent assurance that an organisation's risk management, governance and internal control processes are operating effectively.

- “IAA helps organisations accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”

- “IAA is an important component of *internal control*, *risk management and corporate governance* and provides the necessary assurance and advisory services to the organisation”.

The AGSA points out that internal audit units did not actively follow up the implementation of information technology controls. Internal audits therefore need to consider IT controls in their audit plans.

The Role of Internal Audit in IT Auditing

- IT is an integral part of the organization’s strategy
- It cannot be separated from the accomplishment of organizational objectives
- ITGCs have to be evaluated on a regular basis like other internal controls
- Evaluation requires a CISA qualification
- CISA qualification can be obtained through Information Systems Audit & Control Association

Basic Advisory Role

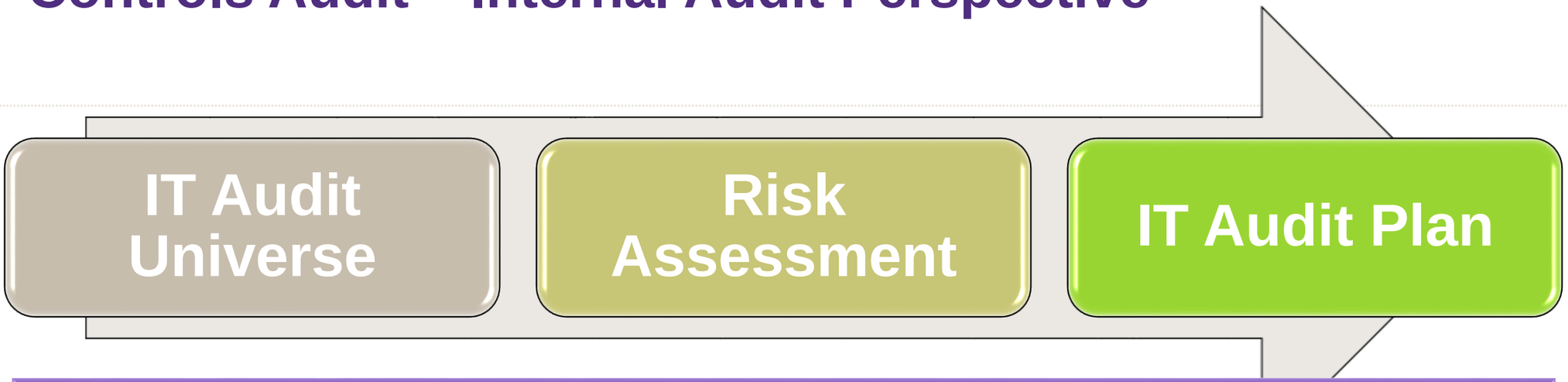
Basic IT Controls

SNG Grant Thornton

An instinct for growth™

Embracing IT Audits

IT Controls Audit – Internal Audit Perspective



- **Understand the business:**
  - **strategy & objectives (IDP)**
  - **structure of municipal operations (key business areas & high risk areas)**
  - **regulation & compliance requirements**
- **IT support model (centralized/decentralized, outsourcing, customization, cloud etc)**
  - **application systems**
  - **critical infrastructure**
  - **major projects & initiatives**

Identify risks, assess and prioritize risks; Understand the universe of potential audit

Risk assessment and control enablers

ISACA identifies 8 control enablers for supporting good governance and accomplishing organizational goals and delivery of stakeholder value:

- Principles,
- Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

ITGCs and ITACs Risks

- Lack of IT governance
- Lack of / unapproved / inadequate policies and procedures
- Identity and access management
- Lack of IT skills and competencies
- Old IT infrastructure
- Segregation of duties
- Unauthorized changes: master files, systems, programs
- Loss of data;
- Unavailability of data
- Inadequate design of manual & automated controls
- Errors in transaction processing
- Poor or inadequate vendor management

Emerging IT Risks

- Cloud computing
  (dependency on third party, reliance on internet, compliance with laws and regulations)
- Mobile devices
  (laptops; tablets; cellphones etc)
- Social networking
- Risks from IT innovations
- Cyber security risk (ransom attacks, denial of service etc)
- Data privacy risks (POPI readiness and compliance)
- Project delays or failure

IT Control Testing

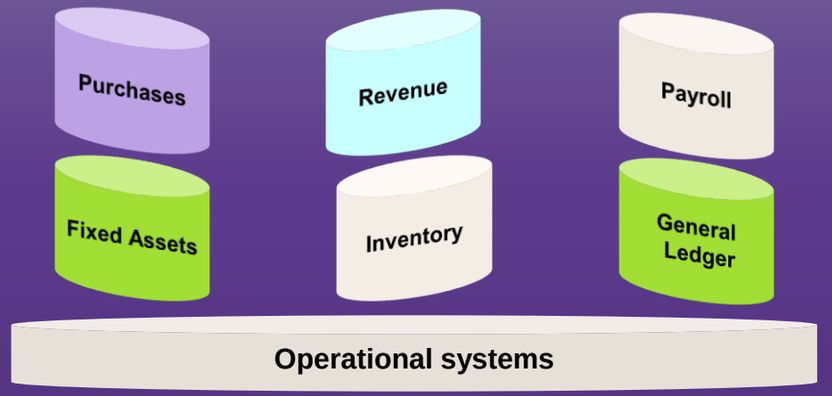
IT Controls

General Controls

- IT Governance
- Security Management
- Data Centre Management
- Backup & Restore
- User Access Management
- Change Management
- Problem & Incident Management

Applications (Input, Processing & Output Controls)

- Authorization
- Integrity
- Segregation of duties
- Availability
- Confidentiality



Application, Database, Network, Operating System

Risk Based Internal Audit Plan Including IT

IT Control Testing

IT Governance:

- MCGICT policy (IT governance structures, TORs,)
- IT strategy alignment to IDP; IT innovation to enable service delivery e.g Wi-Fi
- IT organizational structure in relation to IT strategy
- Allocation of IT roles and responsibilities
- IT assets
- IT budget
- Performance measurement (IT division)
- Performance measurement (IT Vendors)
- Value realization on IT projects
- Risk management

IT Control Testing

Disaster Recovery Planning

- BCP – services offered by the municipality (not an IT responsibility)
- BCP and DRP alignment

User access management

- Identifiable users
- User access matrix
- Comprehensive user listings showing user creation dates; termination dates; indicating any changes done on user credentials
- User deregistration (link to exit process; link to AD)

Key audit considerations

- Timing of the internal audit
- Risk based audit approach (comprehensive IT risk assessment)
- Follow up on implementation of action plans (previous audit reports)
- Develop a risk and control matrix
- Evaluate ITGCs & ITACs control design
- Evaluate ITGCs & ITACs control effectiveness
- Document and discuss deficiencies
- Analyze the root cause
- Advise management on action plans
- Consider the use of data analytics where appropriate particularly on ITACs

Guidance for auditing

- ISO series
- MCGICT policy
- COBIT 5 enabling processes
- IIA practice guides
- IIA standards
- ISACA standards

SNG Grant Thornton

An instinct for growth™

Collaboration on ITGCs & ITACs

Clean Audit Initiatives

Assurance

- IT audit training for internal audit staff
- Perform IT audits with internal audit:
  - IT general controls review
  - IT application controls review
  - IT governance review
  - Data migration review
  - IT security reviews (penetration testing, vulnerability assessments)

Co-sourced approach to foster skills transfer

Advisory

- IT risk assessment
- IT audit readiness
  - Implement IT processes
  - Train IT departments staff
  - IT training for non – IT managers
  - Develop policies and procedures
  - Develop / implement IT governance framework
  - Develop / implement IT strategy
  - Business continuity planning
  - Business continuity training
  - IT process maturity assessment & POPI readiness assessment

SNG Grant Thornton

An instinct for growth™

Project Assurance

Introduction

Project assurance is about evaluating project performance to confirm that project objectives will be met or were met at the end of the project.

SNGGT project assurance includes:

- Project risk reviews
- Pre-go live reviews
- Project gateway reviews
- Post implementation reviews
- Programme / project governance reviews

Project Risks

- Scope not clearly defined or managed
- Scope overrun, budget overrun, time overrun
- Lack of in-house project management (over-reliance on service providers)
- Lack of project management office (project documentation & monitoring)
- Unclear definition of project roles and responsibilities
- Unclear user requirements
- Misalignment of system with business processes
- Change management / change control
- Missing / overlooked controls
- Insufficient testing plans / test cases
- Lack of security controls

Example of project assurance scope

- Applicable aspects of the SDLC
  - Change control
  - Change testing
  - Internal Controls
  - Security
  - Data migration
- System maintenance and support post go - live

- Project governance
  - Project management office & related project documentation
  - Project steering committee
  - Project timelines
  - Quality of deliverables
  - Project scope
- Change management

Case studies

Industry	Work Performed
Local Government	Our team (IT auditors; CAs and Certified MSCOA practitioners and MSCOA competence trainer) assisted a municipality in evaluating MSCOA deliverables against the set scope and budget. The team reviewed project documentation including the service provider contract, service level agreement and agreed upon deliverables. Payment terms were also reviewed including the allocation of MSCOA related expenditure i.e capitalization of MSCOA costs. Change management and overall project governance was also reviewed.
Aviation	Our team assisted with various reviews during the implementation of an enterprise business system (aviation ERP systems). Our project assurance specialists assisted with the review of project governance, system functionality, security and data migration. Our team provided assurance from very early stages of the project and made recommendation that were successfully implemented by the project team.

Key audit considerations

- Audit involved at the beginning of the project
- Decide at what stages will the audit add value
- Attend project steering committee meetings
- Provide IA feedback to management and governing body
- Scope the audit appropriately
- Evaluate each phase when it is completed
- Consider change management
- Evaluate each stage of the project and provide recommendations on time
- Understand project specifications
- Understand required internal controls
- Provide advice on maintenance and support

Project success

- Business objectives are met (value / benefits realised)
- Project documentation is document
- Visible project direction, guidance & monitoring
- Project timelines are met
- Project scope is contained
- Project budget is not exceeded
- Quality deliverables
- Business rules / controls are embedded
- Security controls are embedded
- System usage
- System maintenance & support

Recent statistics on project governance gaps – UK study

Defined project methodology	• 60% applied it mostly / always
Scoping document at planning	• 59% created it mostly / always
Baseline for project schedules	• 48% mostly / always baselined
Project risk management	• 62% mostly / always engage in it

Significant numbers were not applying these basic project management principles; about 28% never creating scoping document; about 35% not baselining project schedules

Clean Audit Initiatives on project assurance

- Provide experienced auditors to work with internal audit
- Perform the audits on behalf of internal audit
- Identify gaps at each stage of the project
- Discuss gaps with relevant process owners
- Prepare audit report
- Provide insight on recommendations and action plans

SNG Grant Thornton

An instinct for growth™

Data Analytics

IT Audits and Advisory

As part of internal audit assignments and/or one-off reviews we have undertaken numerous engagements, using Computer Assisted Audit Techniques (CAATs) to help our clients analyse the details behind their data and implement continuous monitoring . IT should be considered on revenue management to assist the municipality in the following areas:

- Data cleansing e.g duplicate accounts, missing accounts, active/inactive accounts, invalid / incorrect addresses.
- Correct classification of accounts, e.g government, business, residents etc.
- Identify accounts which are not billing all services
- Identify accounts with incorrect billing codes/tarrifs, e.g property registered as business property however levied/billed as a residential property
- Identify incomplete customers details (i.e Names, postal address, contact details and physical address)

Questions

?