Mpumalanga Internal Audit Retreat

Reputation promise/mission

The Auditor-General of South Africa has a constitutional mandate and, as the Supreme Audit Institution (SAI) of South Africa, it exists to strengthen our country's democracy by **enabling oversight, accountability and governance** in the public sector through auditing, thereby **building public confidence.**

Scope and layout of the presentation

- Purpose of existence of Information Systems Audit
- Information Systems Audit Services
- ISA Methodology
- Information Systems Audit Scope
- Information Systems Audit GCR Scope – Financial and Performance Information Systems
- Information Systems Audit Scope – Process Reviews For Performance Information Systems

- Analysis of IT Controls Weaknesses
- Assessment of Key Coordinating Departments/Bodies
- Status of ISA Findings
- Audit outcomes
- Recommendations to management (controls to be designed, implemented and sustained over time)
- What value can Internal Audit add to clean IS audit findings

Purpose of existence of Information Systems Audit

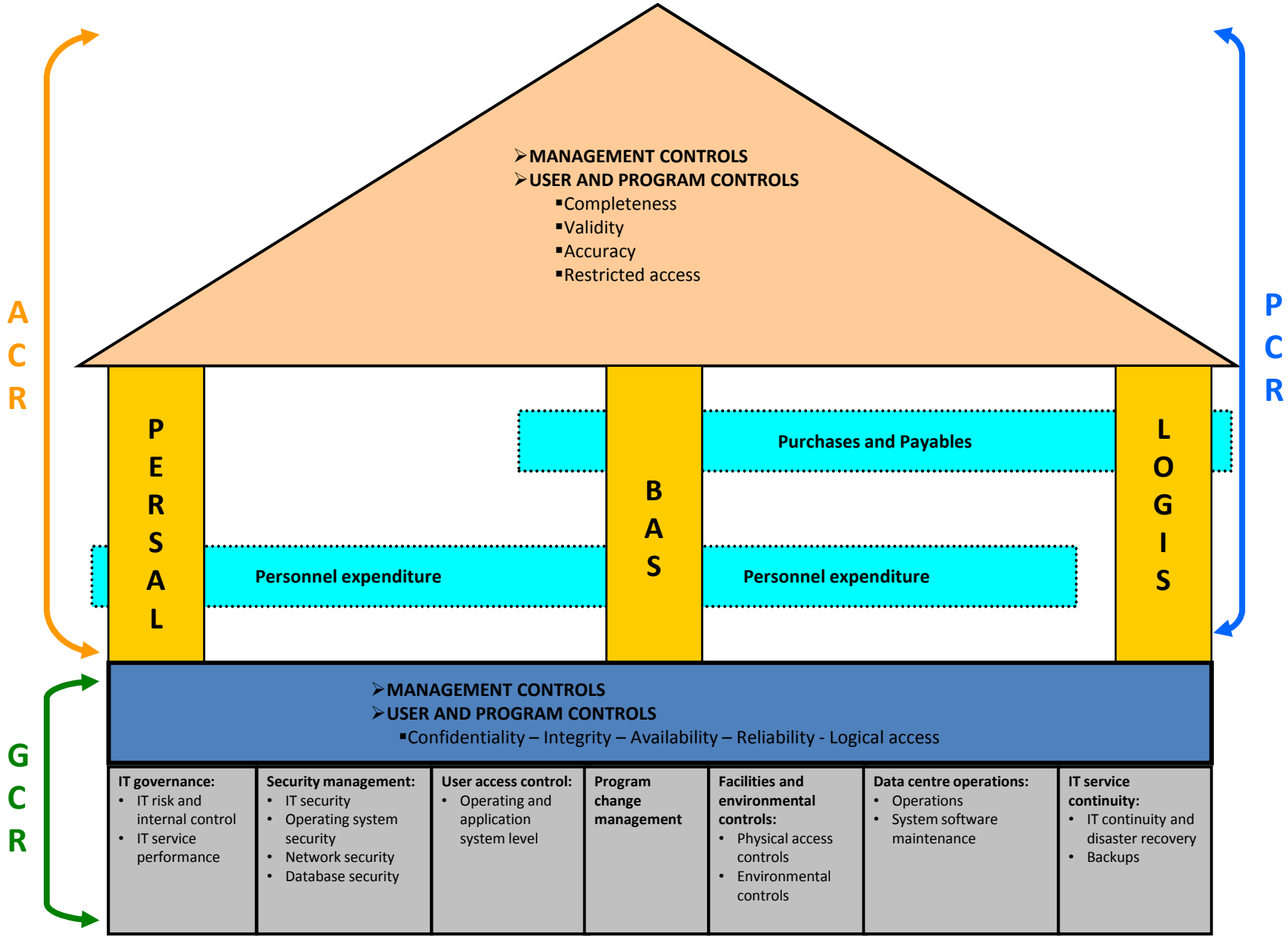
	Planning	Execution	Reporting
RA	•Audit strategy • Action plans •Contact meetings	Provide support to ISA	•Obtain management comments • Include IT findings in management reports
ISA	•Input to audit strategy •Attend contact meetings • Request for Information •Planning risk register •CIS environment of applications with financial impact	•Meetings with officials • Assess audit evidence • Preliminary list of findings	•Discuss and clear the findings with management • Prepare final risk register •Update the key control dashboard

Information Systems Audit Services

ISA audits in support of the Regularity Audit financial statement and predetermined objectives audit. The following audits are performed by ISA:

- GCRs
- Process reviews
- ERP basis reviews
- ERP process reviews
- Network risk assessments
- Full network audit reviews
- AOPO GCRs
- AOPO process reviews
- Project assurance
- Data analytics (CAATs)
  - Transversal systems
  - COI
  - Other systems
  - CAATs on data migrations (New systems)
  - Specific CAATs requested by RA


ISA
Methodology


➢MANAGEMENT CONTROLS
➢USER AND PROGRAM CONTROLS
▪Completeness
▪Validity
▪Accuracy
▪Restricted access
ACR
PCR
PERSAL
BAS
LOGIS
Purchases and Payables
Personnel expenditure
Personnel expenditure
➢MANAGEMENT CONTROLS
➢USER AND PROGRAM CONTROLS
▪Confidentiality – Integrity – Availability – Reliability - Logical access
GCR
IT governance:
• IT risk and internal control
• IT service performance
Security management:
• IT security
• Operating system security
• Network security
• Database security
User access control:
• Operating and application system level
Program change management
Facilities and environmental controls:
• Physical access controls
• Environmental controls
Data centre operations:
• Operations
• System software maintenance
IT service continuity:
• IT continuity and disaster recovery
• Backups

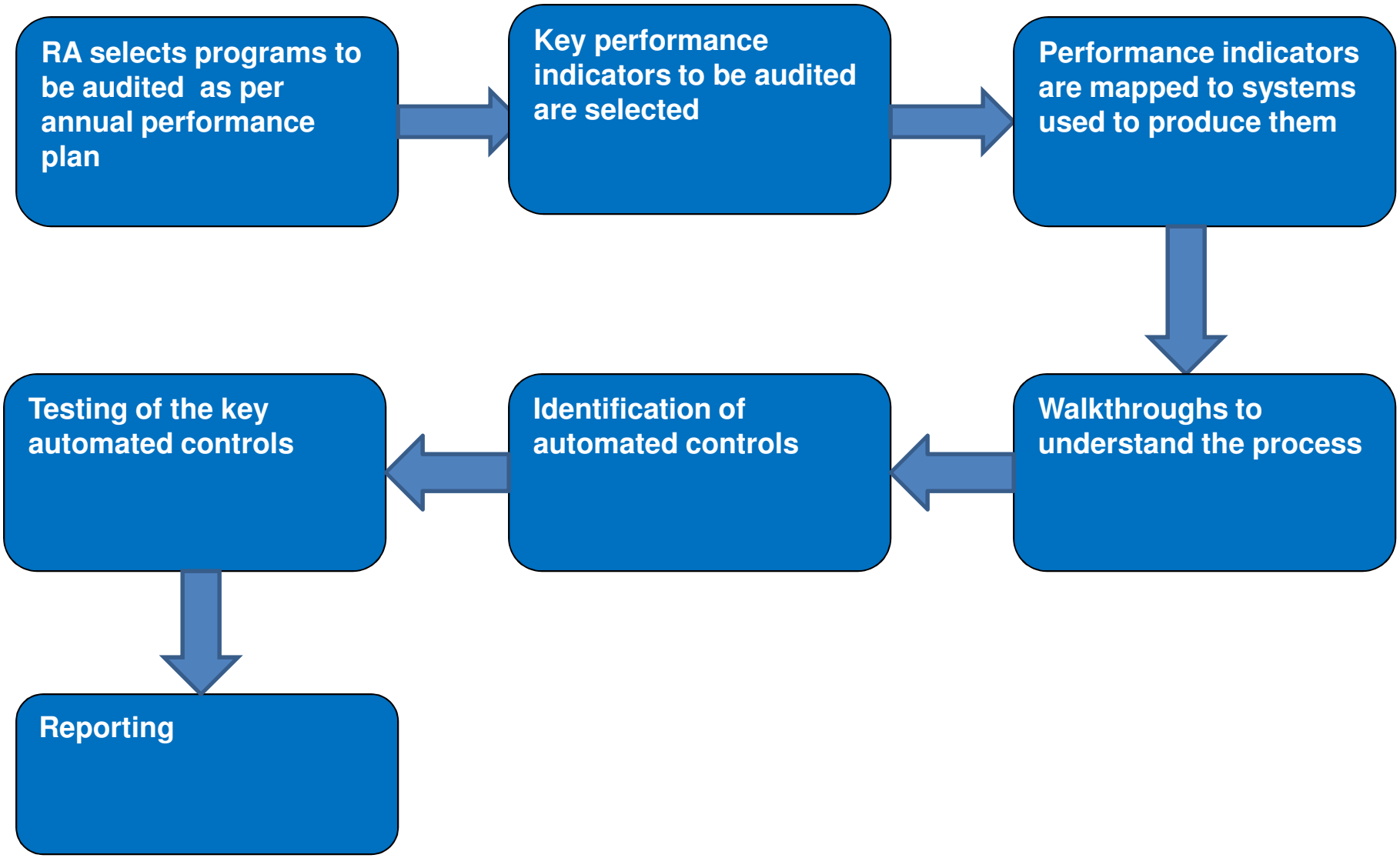
Information Systems Audit Scope

Status of state information	**Confidentiality** The necessary level of secrecy is enforced for all state information. This will be ensured by auditing the following focus areas: • Security Management • User Access Controls	**Integrity** unaltered until authorised to change and is complete. This will be ensured by auditing the following focus areas: • User Access Controls • Data analytics	**Availability** All state information is ready for use when expected. This will be ensured by auditing the following focus areas: • IT Continuity • Security management
Status of key enabling controls	Good governance		
	Effective management		
	Secure architecture / infrastructure		

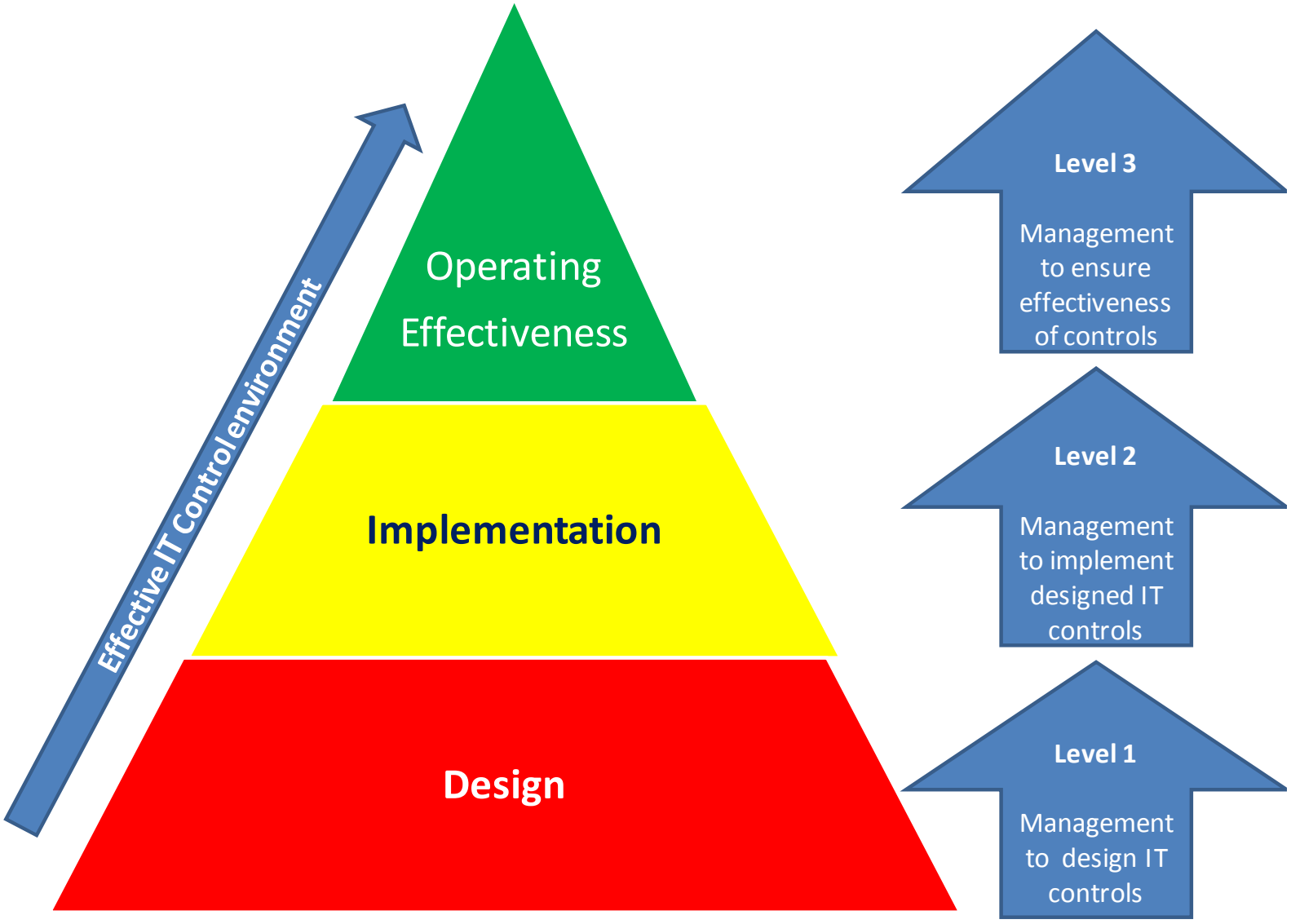
Information Systems Audit GCR Scope – Financial and Performance Information Systems

Focus area	Transversal	Non-Transversal
IT Governance	Department	Department
Security Management	Department (security) Department (network) SITA (OS - mainframe)	Department (security) Department (network and OS)
User account management	SITA National Treasury Department	Department National Department
Program change management	National Treasury	Department National Department
Facilities and environmental controls	Department SITA	Department National Department SITA
Data centre operations	SITA	Department National Department
IT service continuity	Department (DRP/BCP SITA (DRP)	Department National Department

Information Systems Audit Scope – Process Reviews For Performance Information Systems



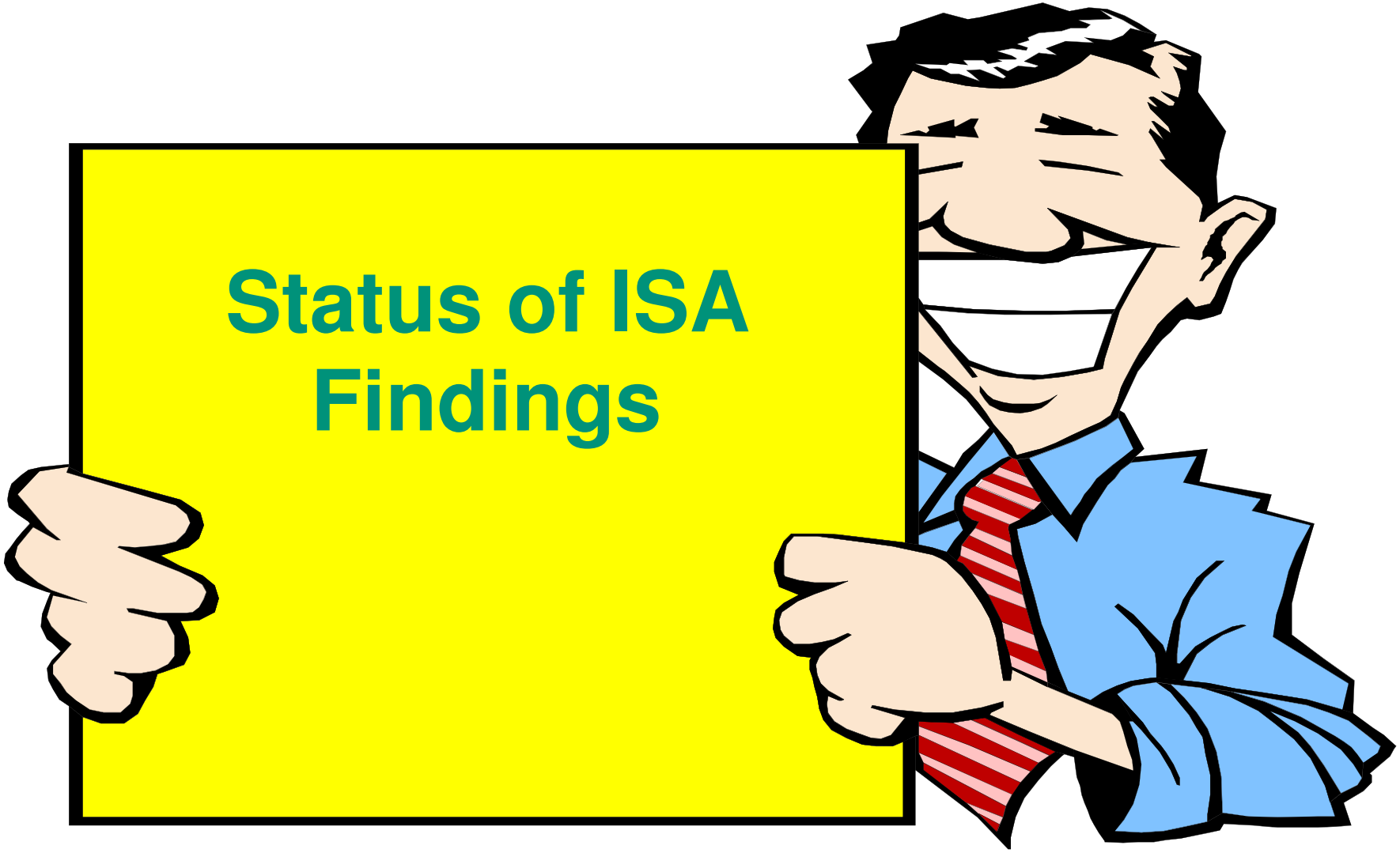
Analysis of IT Controls Weaknesses



Assessment of Key Coordinating Departments/Bodies

Department of Finance	• Super system controllers that managed user access on BAS, PERSAL and LOGIS systems • Provide a transversal user account management policy for implementation and compliance by departments • Network security management
Office of the Premier	• IT Governance framework • Should drive the central development and implementation of policies
COGTA	• Should provide support to municipalities
Internal and Audit Committee	• Track audit findings • Provide management assurance

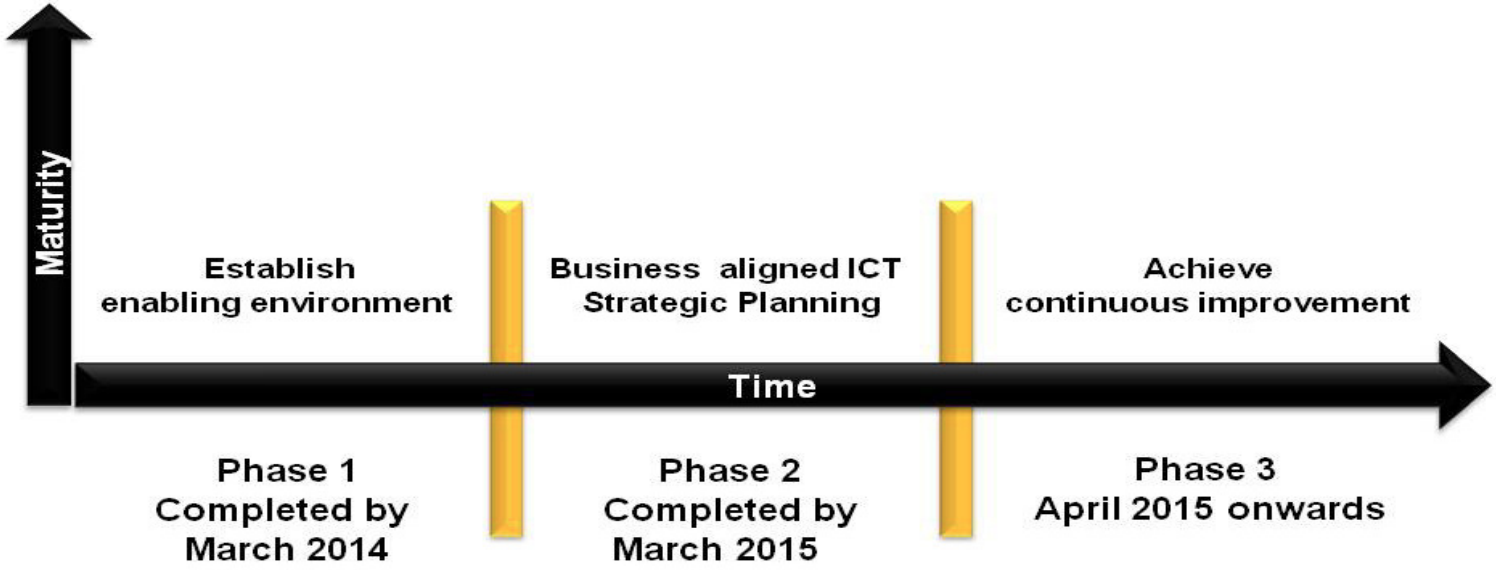
Status of ISA Findings



Status of ISA Findings

IT Governance (Implementation will be audited after March 2014)

- IT governance framework
- Service level agreements (SLAs)
- Monitoring of performance in terms of SLAs
- IT risk assessment and IT risk register
- IT strategic plan
- IT steering committees



Status of ISA Findings

Security management

- Responsibility for information security officer (Departments / Entities = 2)
- IT security policy not adequately designed and not approved (Departments / Entities = 10)
- Operating system standards and procedures (Departments / Entities = 1)
- Operating system security policy settings (Departments / Entities = 1)
- Network security (Departments / Entities = 7)
- Database security (Departments / Entities = 1)

Status of ISA Findings

User access management

- Policy, standards and procedures not adequately designed and not approved (Departments / Entities = 12)
- User access request documentation (new user, password resets, modification of access rights, termination of access) (Departments / Entities = 5)
- Reviews of appropriateness of users' access rights (Departments / Entities = 11)
- Reviews of system administrator activities (Departments / Entities = 12)
- Accountability of user IDs (Departments / Entities = 1)
- Segregation of duties (Departments / Entities = 9)
- Password security settings (Departments / Entities = 3)

Status of ISA Findings

Program change management

- Policy, standards and procedures (Departments / Entities = 3)
- Monitoring of access to the production and test environment by an independent person (Departments / Entities = 1)
- Migration of changes to the production environment (Departments / Entities = 1)
- User acceptance testing (Departments / Entities = 1)

Status of ISA Findings

Facilities and environmental controls

- Access to server rooms (Departments / Entities = 1)
- Request for access to server rooms (Departments / Entities = 1)
- Periodic review of access to server room (Departments / Entities = 1)
- Regular maintenance on environmental controls (Departments / Entities = 2)
- Inadequate environmental controls (Departments / Entities = 1)

Status of ISA Findings

IT service continuity

- Business Continuity Plan and Disaster Recovery Plan (Departments / Entities = 10)
- Testing of Disaster Recovery Plan (Departments / Entities = 1)
- Participation in the testing of the SITA mainframe disaster recovery plan (Departments / Entities = 11)
- Backups standards and procedures (Departments / Entities = 4)
- Testing of backups (Departments / Entities = 1)

Audit outcomes

- The audit outcomes indicated that the majority of departments experienced challenges with the design and implementation of IT controls.
- Adequate progress had not been made in addressing previous findings as risks remained in some of the focus areas, even though some corrective measures had been instituted.
- The lack of adequate progress could be attributed to inadequate oversight by those charged with governance, a lack of consequences for not resolving audit findings and a lack of consistent monitoring by internal audit and audit committees of the progress made in implementing management commitments.

Recommendations to management (controls to be designed, implemented and sustained over time)

- Executives should buy into the adoption of the IT governance framework developed by DPSA.
- Management should ensure that development plans are established for up skilling their IT staff.
- Oversight departments should prioritise oversight responsibilities at departments that are lacking in adequately designed controls.
- Vacant positions that have been approved should be filled.
- The provincial GITO, through COGTA, should facilitate knowledge sharing regarding the importance of IT with departments' and municipalities' management.
- PGITO meetings should be extended to include municipalities to enhance the sharing of knowledge at IT management level.
- Internal audit at departments and municipalities should extend their scope to include IT audits.
- Audit committees should play an oversight role to ensure that IT risks are appropriately managed.

What value can Internal Audit add to clean IS audit findings

- Combined assurance (ISA 610)
  - Planning of audits
  - Scope of audits
  - Timing of audits (PFMA before October)
- Capacitate Internal Audit with information systems auditing skills
- Train Internal Audit on information systems auditing
- Coordinate and monitor action plans / project plans on ISA reports
- Coordinate and monitor progress on addressing risks and findings in the dashboard reports / key control documents

Questions? comments