Session date

Session subject

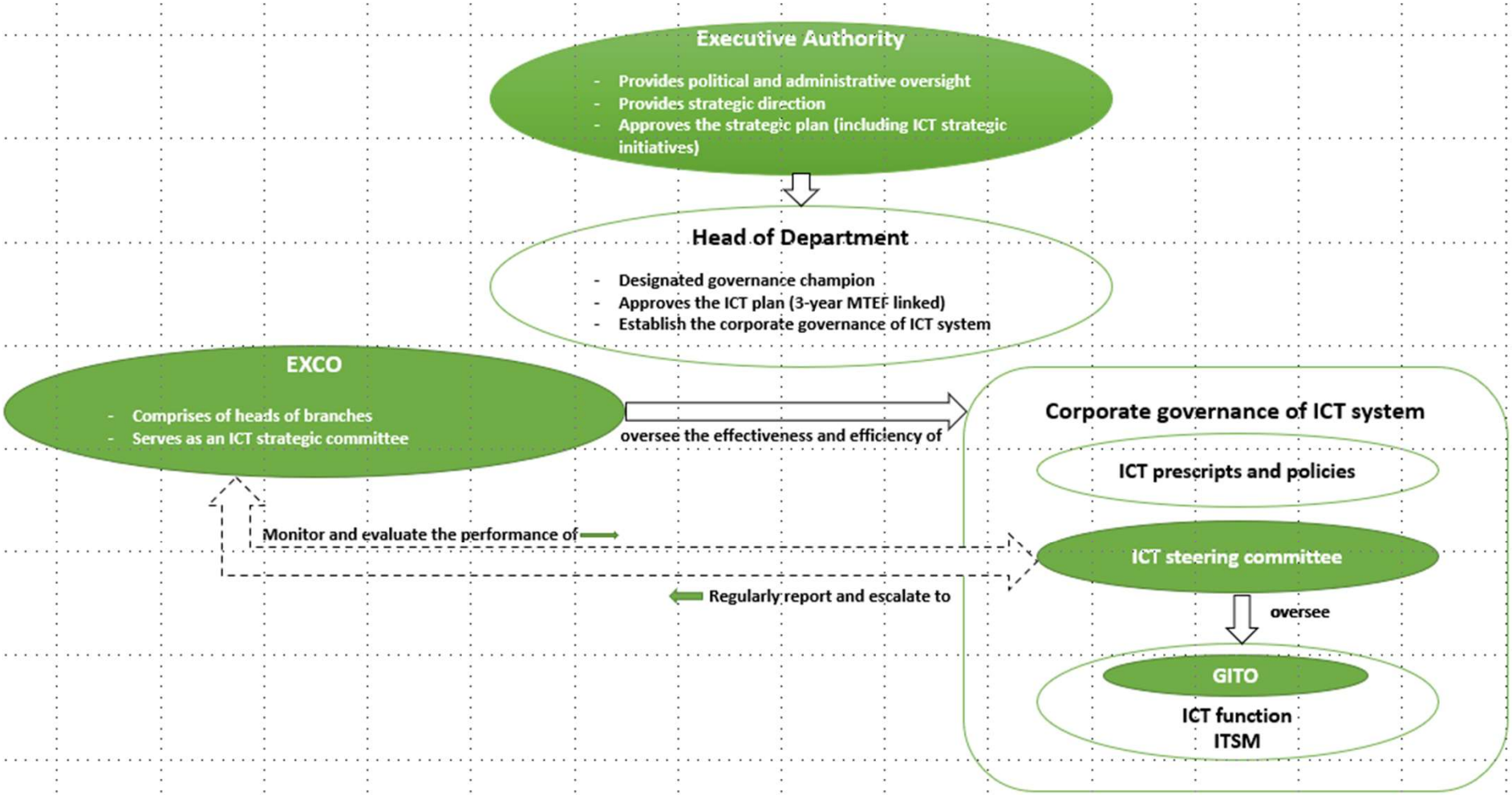
CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Aubrey Mochela
City of Johannesburg

Corporate Governance of ICT
Critical Instrument for Data Protection and Compliance

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Corporate Governance of ICT

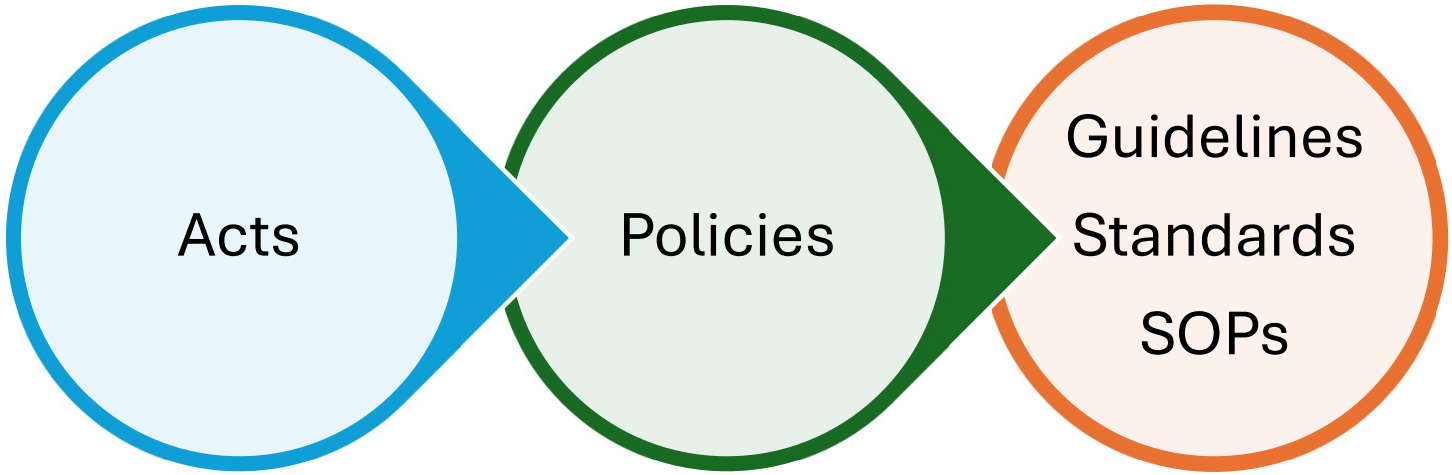


Policy Universe

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Business Area	Governing Act / Regulation	Government Framework	Strategy & Business Plan	Policy Level1	Policy Level2	Policy Level3
Office of City Manager	MFMA MSCOA BCE CompanyAct ICASA POPI PAIA ICASA ECT CyberSec	MFMA	CoJ IDP SDBIP BP SDBIP BP	StakeholderPolicy		
COO (Core Business Ops, Projects)		CGICTPF SPMO	CGICTPF COJ ICTGF ICTStrat InfoSecPlan ICTCMPlan	Policies for DM PMO AU InfoSec ITSM IM CM ICTCM Cloud	ITIL COBIT PMI TOGAF	
Management Support (HR, Internal IT, Facilities, Security)			ManSuppStrat FacilitiesPlan PhysicalSecPlan	HRPolicies ICT Policies	ICTSLA	CoC HRForms BSSQP
Legal (Contracts)				LegalPolicy	Contract Templates	Contracts
Finance (Fin, Asset, SCM)		MFMA PPP Framework	FinStrat AssetPlan	SCMPolicy AssetPolicy	SCMValueChain	SCMFroms SCMSOPs SCMTemplates
Governance Risk & Compliance		ERM Framework PolicyFrawork PolicyUniverse ReportingFW	RiskStrat RiskPlan	RiskPolicy		
Audit		MFMA	AuditStrat AuditPlan	AuditPolicy		

CoJ Cyber-Security Strategy



Strategy

Plans

CoJ Smart City Ecosystem

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Safe, Sustainable, Convenient, Prosperous and Resilient

where all citizens have access to services and information, which enhances socioeconomic development and service delivery

City Brain

Management Panel | Economic situation | Event Management | Service Management | Decision Making Support | ...

One Application

- Smart Power infrastructure
- Smart Water infrastructure
- Safe City- Infrastructure protection
- Smart Planning (Digital Twin)
- Consolidated IT Systems

One Enable Platform

- AI Enable
- Big Data
- Internet of Things
- Integrated Communication Platform

One Cloud

- Cloud

One Network

- Connectivity-Done

Data Protection at City of Johannesburg

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Data Protection Approach using DLP

- DLP Tool that has been operating successfully in the City of Johannesburg environment for over a year, safeguarding thousands of endpoint devices without any end-user intervention.
- The solution delivers comprehensive visibility and control to ICT data environment—allowing the City to define what data is backed up, where it's stored, and when protection occurs.
- Tried, tested, and fully operational and was rapidly deployed and has consistently demonstrated its functionality, ease of use, and significant impact on data protection for COJ endpoints.

Data Protection Approach using DLP

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

85% of breaches result from social engineering tactics, such as phishing and pretexting scams.

More than **70%** of data loss incidents originate from employee endpoints.

There is a **fundamental security flaw** in the way email was designed.

91% of cybercrimes start through accessing email.

Microsoft Service Agreement

6. Service Availability

b. ... We recommend that you regularly backup the Content and Data that you store on the Services or store using Third-Party Apps and Services.

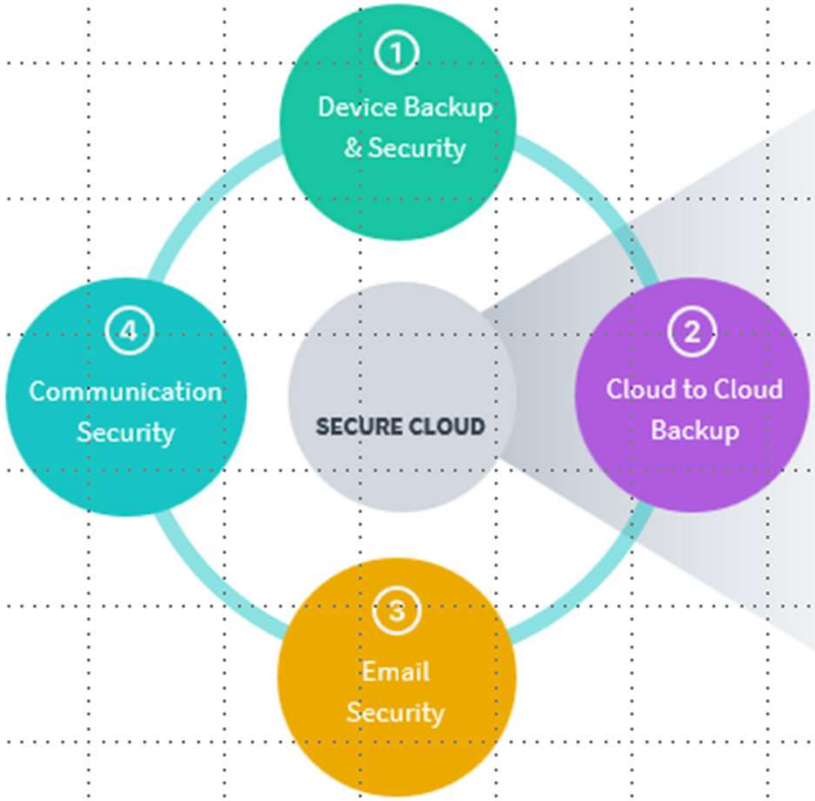
https://www.microsoft.com/engb/servicesagreement/

Simple Steps to follow for DLP

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Secure Your Data Using Cloud

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



1. **Device Backup & Security**
   - Backup
   - DLP
   - Migration
2. **Cloud to Cloud Backup**
   - O365
   - SaaS Backup
3. **Email Security**
   - Advanced Threat Protection
4. **Communication Security**
   - DMARC

Critical Tool Box to use for Data Protection

Tool Box

[1] Cybersecurity Strategy which has a section on overall guideline on how to handle data governance

[2] The City did a POPIA compliance assessment with the CSIR. This helps understand where the gaps are in terms of compliance and the team then implemented technical controls to address the gaps.

[3] Data Governance Policy

[4] Information and Cybersecurity Policy

Tool Box

[5] Cloud Computing Policy

[6] GICT Priority Regulatory Register (risk rigister)

[7] Full disk encryption for hard drives, USBs and laptops with Microsoft BitLocker

[8] Data Loss prevention with Netskope (physical devices) and Microsoft Purview (cloud workloads)

[9] Access control to data through multifactor authentication.

[10] 24/7 monitoring and response to cybersecurity incidents

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body