Cyber Security Beyond IT

Governance, Risk, Compliance and Accountability in the Public Sector

Mr Robinson Shai | Guest Speaker | 18 June 2026

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Opening Thesis

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

The governance lens

1. Cyber risk is business risk, service-delivery risk and accountability risk.

2. ICT can operate controls, but leadership must set direction, fund priorities and demand assurance.

3. A cyber incident can become a POPIA issue, a MFMA control failure, a reputational crisis and an audit matter.

4. The question is not only: are we secure? It is: can we prove we are governing cyber risk responsibly?

Agenda

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

1. Cybersecurity as a governance and leadership responsibility
2. Frameworks, legislation and accountability expectations
3. Artificial intelligence: opportunity, risk and controls
4. Readiness assessments, assurance and resilience indicators
5. Practical roadmap for improving public sector cyber resilience

Why Cybersecurity Is Beyond IT

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

It affects the institution, not only the network

Service Delivery

Disrupted billing, licensing, grants, public portals, clinics, libraries or municipal services.

Public Trust

Loss of confidence where personal records, financial data or citizen services are compromised.

Financial Control

Fraudulent payments, supplier compromise, unauthorised changes and weak segregation of duties.

Legal Compliance

POPIA, Cybercrimes Act, records management, procurement and financial governance obligations.

Operational Continuity

Backup, recovery, crisis management and the ability to operate during technology failure.

Accountability

Leadership must demonstrate oversight, risk treatment, monitoring and consequence management.

Sources reflected in speaker notes: South African Government, Information Regulator, ISO and National Treasury / AGSA public materials.

The Accountability Model

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Who owns what?

Council / Board
Sets governance expectations and receives assurance

Accounting Officer
Owns institutional accountability and risk acceptance

Executive Management
Prioritises, funds and monitors cyber risk treatment

ICT Management
Operates controls and provides evidence

Risk, Audit & Assurance
Tests, challenges and reports control effectiveness

Cyber risk is governed through ownership, evidence, assurance and consequence management.

Leadership Responsibilities

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Minimum Cyber oversight questions leaders should ask

1. Do we know our critical systems, data assets and high-risk third parties?
2. Is cyber risk formally captured, rated, treated and reported through the risk governance process?
3. Are minimum controls defined for identity, backups, patching, email security, endpoint protection and logging?
4. Do we have tested incident response and disaster recovery arrangements?
5. Are audit findings, vulnerabilities and control gaps tracked to closure with accountable owners?
6. Do we receive assurance, or only activity reports?

Public Sector Cyber Risk Landscape

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Common risk themes in municipalities and public entities

Legacy Environments

Unsupported systems, shared accounts, unmanaged endpoints and weak asset visibility.

Identity Weaknesses

No MFA, excessive privileges, dormant accounts and poor joiner-mover-leaver controls.

Supplier Exposure

Outsourced ICT, cloud platforms, vendors and consultants with privileged access.

Data Protection Gaps

Unclear data ownership, poor retention practices and weak monitoring of sensitive records.

Sources reflected in speaker notes: South African Government, Information Regulator, ISO and National Treasury / AGSA public materials.

What the Auditor-General's 2024-25 Report Tells Us

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Evidence that cybersecurity is now an audit, governance and accountability issue

70

Auditees assessed

AGSA assessed cybersecurity controls across national and provincial auditees.

45 / 64%

Had shortcomings

Cybersecurity control weaknesses were reported at most auditees assessed.

8 / 11%

Significant vulnerabilities

Some auditees exhibited vulnerabilities that could be exploited if not remediated.

R12.1bn

ICT projects with findings

AGSA evaluated ICT projects and found governance and delivery weaknesses.

Common cybersecurity weaknesses

- Backups not securely and regularly tested
- Weak access controls and password practices
- Unpatched systems and poor vulnerability management
- Insufficient logging and monitoring of administrator activity

Governance message

The AG report reinforces the core theme: cyber risk is not only a technical exposure. It affects service delivery, financial reporting, internal control, public trust and executive accountability.

Frameworks and Laws: One Governance System

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Avoid treating each requirement as a separate project

Requirement	Governance expectation	Practical evidence
NCPF	National coordination, capability and cybercrime response posture	Cyber strategy, incident escalation, awareness and response roles
Municipal ICT Governance	ICT governed as part of corporate governance	ICT charter, committees, policies, reporting and accountability
POPIA	Lawful and secure processing of personal information	Information officer, safeguards, breach handling and operator controls
Cybercrimes Act	Prevention, reporting and response to cyber offences	Incident procedures, evidence preservation and escalation
ISO/IEC 27001	Risk-based information security management system	Risk assessment, controls, internal audits and continual improvement

Legislative Compliance Is Not Paperwork

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Cybersecurity It must translate into operating controls

1. POPIA requires responsible processing and appropriate security safeguards over personal information.
2. Cybercrimes obligations require institutions to identify, escalate and preserve evidence for cyber offences.
3. ICT governance frameworks require clear leadership structures, policies, roles and oversight.
4. Compliance evidence must be current, testable and linked to accountable owners.
5. A policy without operational proof is weak assurance.

MFMA, Risk Management and Internal Control

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

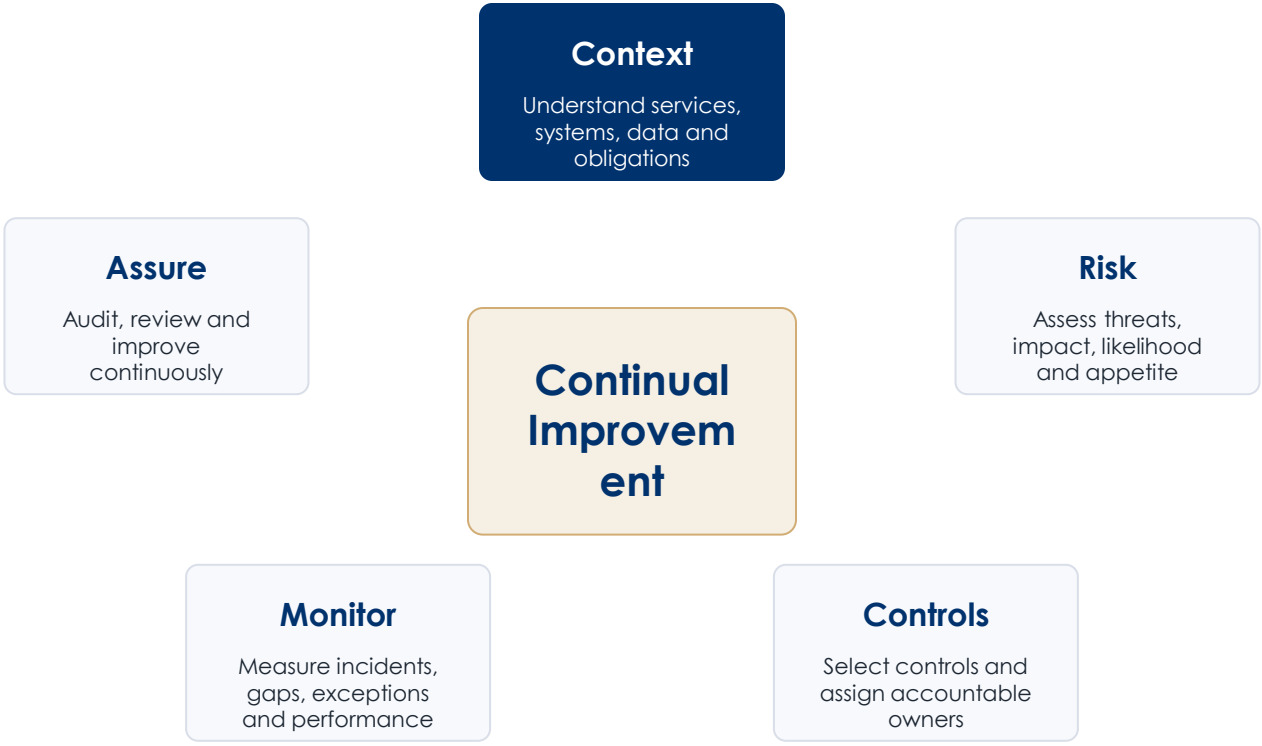
Cybersecurity supports financial governance

1. Financial systems, supplier master data, payroll, banking details and procurement workflows are cyber-sensitive assets.
2. Weak access control can become unauthorised, irregular, fruitless or wasteful expenditure risk.
3. Cyber incidents can impair credible financial reporting and continuity of financial operations.
4. Risk treatment must be budgeted, prioritised and monitored like any other material institutional risk.
5. Consequence management should apply where control failures are ignored or repeated.

ISO/IEC 27001 as an Operating System

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

A practical cycle for managing cyber risk



Artificial Intelligence: Public Sector Opportunities

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

AI can improve capacity, but governance must lead adoption

Citizen Services

Faster query handling, document triage, language support and improved service-channel responsiveness.

Internal Efficiency

Summarisation, drafting, case routing, reporting support and knowledge management.

Risk Intelligence

Pattern detection, anomaly analysis, fraud indicators and earlier warning signals.

Cyber Defence

Alert triage, phishing analysis, vulnerability prioritisation and incident response support.

Sources reflected in speaker notes: South African Government, Information Regulator, ISO and National Treasury / AGSA public materials.

AI Cybersecurity and Governance Risks

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

The risks are new, but the accountability is familiar

1. Sensitive personal information may be entered into tools without proper approval or retention controls.
2. AI outputs may be inaccurate, biased or unsupported, yet still influence public decisions.
3. Staff may use unsanctioned AI tools, creating shadow IT and data leakage exposure.
4. Attackers can use AI to improve phishing, impersonation, social engineering and malware development.
5. Procured AI systems may introduce third-party, cloud, data residency and model-governance risks.

AI Accountability Controls

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Minimum controls before scaled adoption

1. Define approved AI use cases and prohibited data use.
2. Classify data before it is used in AI tools.
3. Require human review for decisions affecting rights, services, finance or compliance.
4. Assess suppliers for privacy, security, data residency and auditability.
5. Log AI-assisted decisions and retain evidence for review.
6. Include AI risks in the institutional risk register and assurance plan.

Cybersecurity Readiness Assessment

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

What should be assessed?

Domain	What to assess	Typical evidence
Governance	Structures, policies, roles, reporting and risk ownership	Terms of reference, minutes, dashboards, approvals
Identity	MFA, privileged access, user lifecycle and access reviews	Account lists, review evidence, admin role register
Technology Hygiene	Asset inventory, patching, endpoint security and vulnerability management	Scan results, patch reports, EDR coverage
Resilience	Backups, recovery tests, incident response and crisis communications	DR test reports, playbooks, restoration evidence
Assurance	Internal audit, risk monitoring and combined assurance coverage	Audit plan, findings tracker, assurance map

Key Indicators of Cyber Resilience

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Metrics leadership can understand

Control Coverage

Percentage of endpoints protected, identities with MFA, systems logged and critical assets backed up.

Response Capability

Time to detect, time to contain, tested incident playbooks and named response roles.

Recovery Confidence

Successful restore tests, recovery time objectives and backup isolation status.

Remediation Discipline

Age of critical vulnerabilities, overdue audit actions and repeat findings.

Third-party Risk

Privileged supplier access, contract security clauses and assurance over outsourced services.

Governance Rhythm

Cyber risk reporting, committee oversight, exception approvals and consequence tracking.

Internal Audit, Risk and Combined Assurance

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Assurance must test cyber risk, not only policy existence

1. Risk management should maintain cyber risk scenarios, ratings, treatments and accountable owners
2. Internal audit should test control design and operating effectiveness.
3. ICT should provide evidence, not self-assurance only.
4. Legal, compliance, supply chain, records and HR should be included where relevant.
5. Combined assurance should show who gives assurance over which cyber risks and controls.
6. Audit committees should track repeat findings and unresolved high-risk issues.

Common Public Sector Cyber Failures

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Patterns that turn small weaknesses into major incidents

1. Cybersecurity is reported as tool deployment, not risk reduction.
2. Policies exist, but owners, evidence and enforcement are weak.
3. Privileged access is not reviewed and generic accounts are tolerated.
4. Backups are performed but not restored and tested under realistic conditions.
5. Vulnerabilities are scanned but not remediated with deadlines and accountability.
6. Supplier access is granted faster than it is governed, monitored or removed.
7. Incident response plans are written but not exercised with executives

90-Day Governance Roadmap

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

A practical starting point for public sector institutions

0-30 Days

Establish ownership
Critical asset and data inventory
Cyber risk register and top risks
Basic control visibility dashboard

31-60 Days

MFA and privileged access actions
Backup and recovery testing
Incident response roles and playbook
Critical vulnerability closure plan

61-90 Days

Executive cyber risk reporting
Internal audit assurance scope
Supplier access review
Board / council cyber resilience pack

Outcome: visible ownership, tested controls, prioritised remediation and repeatable assurance.

Key Takeaways

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

What leaders should remember

1. Cybersecurity is a governance responsibility before it is a technical function.
2. Compliance must be evidenced through operating controls, not policy documents alone.
3. AI can improve public sector capacity, but it requires privacy, security and accountability guardrails.
4. Readiness must be measured through evidence, resilience indicators and independent assurance.
5. Public sector cyber resilience improves when ownership, funding, monitoring and consequence management are clear.

Thank You!

Questions & Discussion

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body