Auditing Cybersecurity (Topical Requirements)

YAMKELA MEHLOMAKULU - C-CIO(SA)
BCom IS, BCom Hon IT Forensics, MPhil IT Governance,
Doctoral Candidate IT

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

South Africa under cyber threat

Auditor-General Ms Tsakani Maluleke (right)

The AGSA has emphasised that cybersecurity remains a top concern for governments worldwide, especially in South Africa.

Table of Contents

Introduction: Why Cyber Security Auditing Matters in South Africa

- **Threat environment**: Government systems face phishing, ransomware, and credential theft that can interrupt essential services and expose sensitive records.
- **Citizen confidence**: When service portals, payments, and records remain available and trustworthy, citizens experience government as reliable and legitimate.
- **Three spheres**: Audit findings must be relevant across national departments, provincial administrations, and municipalities, each with different maturity and risk.
- **Audit outcomes**: A strong audit clarifies exposure, strengthens controls, and gives leaders a defensible roadmap for remediation and oversight.

Cybersecurity Facts!!!

- The AGSA has emphasised that cybersecurity remains a top concern for governments worldwide, especially in South Africa.
- The Communication Risk Information Centre said in their 2025 telecommunications sector report that cybercrime costs South Africa an estimated **R2.2 billion per annum.**
- 70 of the AGSA's auditees were assessed on the effectiveness of their cybersecurity prevention measures and their vulnerability to cyberattacks.
- These assessments included the testing of department IT systems to determine potential vulnerabilities and defensive capacity.
- The AGSA found 45 of the auditees were vulnerable to cyberthreats, 23 of which were deemed to be high-impact targets.
- The audit found that many of the auditees did not possess sufficient backup capacity, which could leave them vulnerable to significant financial and data losses in the event of an attack.
- They also identified flaws across multiple departments' systems, increasing the risk of cyber threats to these departments.

Source: Auditor General Annual Reports

Cybersecurity AGSA Findings!!!

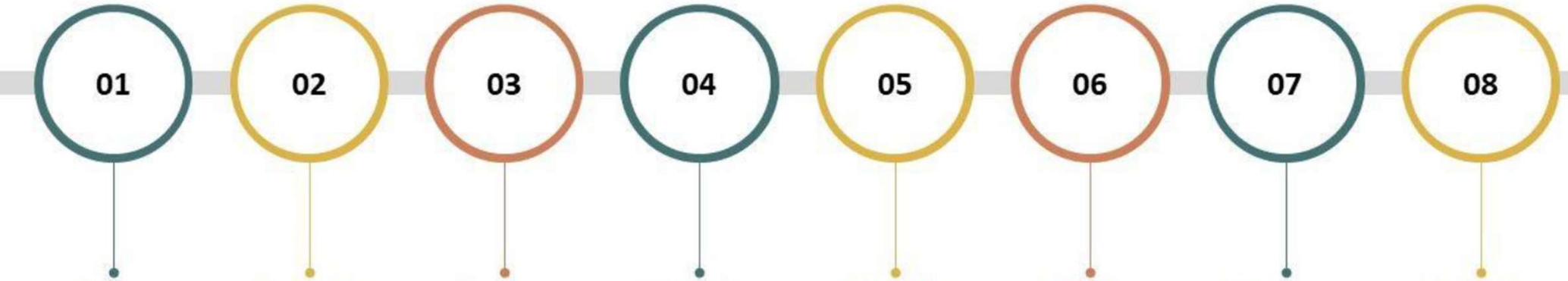
- **Ageing infrastructure:** Auditees did not upgrade outdated IT infrastructure so that it could reliably support key applications. This not only increases the vulnerability to attacks, but also hampers the implementation of modern security measures.
- **Compromised environments:** Security perimeters failed to prevent breaches during penetration testing across multiple environments. This highlights a systemic weakness in the existing defence mechanisms. Several environments were compromised during the year, which had a negative effect on service delivery.
- **Skills deficit:** Most auditees were unable to recruit and retain cybersecurity professionals. The skills gap undermines auditees' ability to proactively defend against and respond to cyberthreats.
- **Third-party risk management:** The risks associated with third-party service providers were not adequately managed. Poor oversight and lax controls expose auditees to potential breaches through their extended networks.
- **Underinvestment in cybersecurity:** Cybersecurity is underfunded, with budgets tied to broader IT expenditure rather than being recognised as a critical business risk. This lack of targeted investment compromises the ability to build robust security programmes

Source: Auditor General Annual Reports

Context, Scope & Objectives of Cyber Security Audits

Information Technology Cyber Audit Planning

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



Define
Identify the scope and objectives of the audit process.

Assemble
Gather a team of skilled professionals for audit execution.

Review
Examine current security policies and compliance requirements.

Identify
Determine key assets and systems to be included in the audit.

Schedule
Create a timeline for the audit, including all major activities.

Notify
Inform stakeholders about the upcoming audit activities.

Prepare
Develop the necessary tools and resources for the audit.

Execute
Initiate the audit process based on the planned approach.

Source: Future Spot

Information Technology Cyber Audit Team

Source: Future Spot

Information Technology Audit Scope & Institutional Landscape

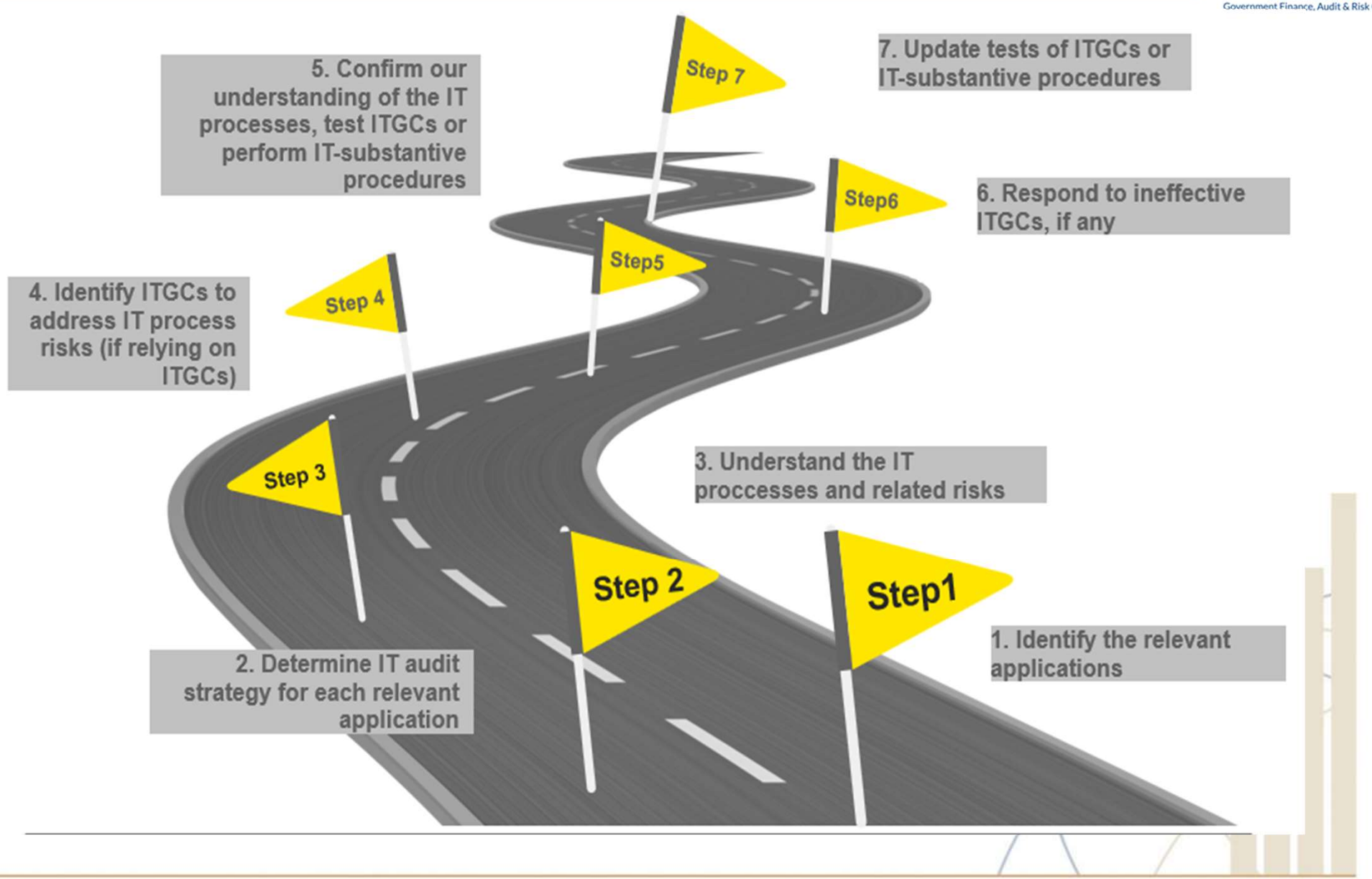
CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

IT Governance	Security Management	User Account Management	IT Service Continuity	Program Change Management	IT Contracts and Projects
• Ensure Governance Framework settings • Ensure Benefits delivery • Risk optimisation • Ensure Resource optimisation • Service Level Agreement	• Approved IT Security policy • Antivirus installed • Patch management process and procedures • Password Configuration • Firewall	• Approved Policy and Procedures • User access forms • Reviewing of users access • Review of system controller activities • Unique user id • Terminations	• Disaster Recovery plans • DRP Test • Backup Policy • Backups performed • Backup restoration • Offsite storage for backups	• Program Change Policy • Change control forms • Testing of Changes • Segregation of duties	• Contract register • SLAs and monitoring • Business case • Project governance

Source: Auditor General Audit Strategy/ Auditor General Annual Reports

IT Audit Road Map:
The steps in performing an IT audit

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



IT Audit Road Map:
Typical IT Process

Manage access

Provide access to the IT environment only to authorized, appropriate users and those users are restricted to performing authorized, appropriate actions.

Manage changes

Make changes to IT application programs and other relevant IT environment components that are appropriate and function as intended

Manage IT operations

Provide a reliable processing environment that is prepared for routine operating issues resulting from the loss of IT application programs and data and the incomplete processing of information

Cyber Security Audit Scope & Institutional Landscape

Defining what is in and out of scope

Government spheres

National, provincial, and municipal entities operate distinct mandates, yet often share platforms, data flows, and procurement dependencies.

Key assets

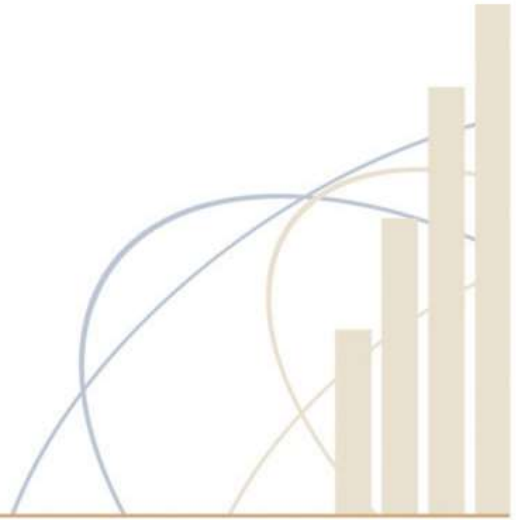
The audit should prioritize identity stores, email, financial systems, citizen databases, endpoints, and cloud services.

Ecosystem

Users, administrators, contractors, managed service providers, and software suppliers all influence the attack surface and control environment.

Audit boundary

Scope must specify systems, locations, periods, interfaces, and exclusions so evidence is complete and engagement risk remains controlled.



Cyber Governance, Accountability & Compliance Landscape in South Africa

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Executive responsibilities and compliance baseline

Item	Details
Executive oversight	Governance bodies must approve risk appetite, monitor remediation, and demand regular reporting on cyber posture and material exceptions.
Role clarity	Security, IT, risk, legal, and internal audit functions need explicit responsibilities to prevent gaps, duplication, and blame shifting.
Compliance	Controls should be tested against the PFMA, MFMA, POPIA, Treasury instructions, and sector-specific directives where applicable.
Policy maturity	A mature environment links formal policies to standards, procedures, metrics, and evidence of consistent operational enforcement.

Audit Objectives: Government

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Define a clear set of audit objectives that cover assurance, compliance, risk reduction and service continuity, ensuring they align with King IV and PFMA/MFMA. Distinguish the scope and depth of internal, external and regulatory reviews. Map objectives to the national cyber security strategy and sector frameworks to support business continuity and critical service delivery.

Planning Cyber Audit Objectives

Executing Cyber Audit Activities

Conduct internal audits to test cyber controls, governance practices and continuity plans against defined objectives. Coordinate with external auditors and regulators to perform independent assessments and oversight reviews. Implement testing of business continuity and disaster recovery capabilities, and document how findings support compliance with King IV, PFMA/MFMA and national cyber security frameworks.

Analyze initial audit findings to refine objectives, focusing on gaps in compliance, governance and resilience. Prioritize enhancements that better support business continuity, disaster recovery and critical services. Align optimization with evolving national cyber strategies and regulatory expectations, ensuring sustained improvement and measurable risk reduction over time.

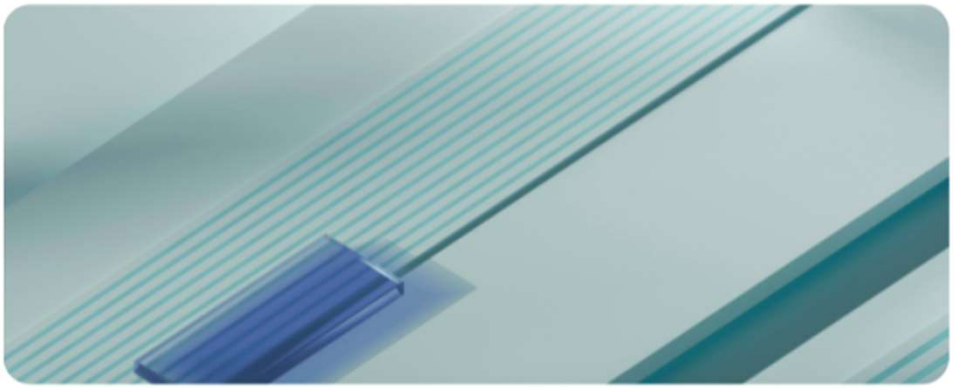
Refining and Optimizing Objectives

Reviewing Audit Outcomes

Evaluate how audit results enhanced assurance, compliance and risk reduction across government services. Assess whether governance expectations under King IV and PFMA/MFMA were effectively supported. Review the performance of internal, external and oversight audits, and how they strengthened continuity, disaster recovery capabilities and alignment with national cyber strategies.

Cyber Governance, Accountability & Compliance Landscape in South Africa

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



Laws, Maturity Gaps & Cyber Threat Exposure

POPIA, Cybercrimes Act, ECT Act, PFMA/MFMA and MISS shape compliance, yet uneven ICT maturity across spheres leaves high-value government entities exposed to increasingly sophisticated cyber attacks.

Government Structure & Central ICT Bodies

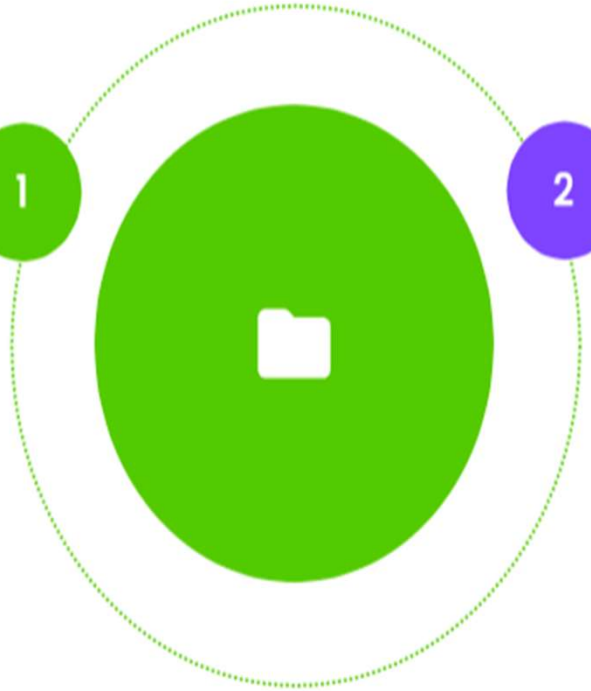
South Africa's national, provincial and local governments coordinate service delivery, while National Treasury, DPSA, SITA and related bodies guide ICT investment, governance standards and cybersecurity alignment.

Audit Scope: Across National, Provincial & Local Spheres

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

1 Defining core scope for cyber security audits

Scope must cover governance, operations, resilience and privacy, while addressing shared services, hosted environments, and inter-governmental platforms across all government spheres.



2 Tailoring depth and approach to each government entity

Audit focus adapts to entity size, mandate, and service criticality, distinguishing enterprise-wide versus system-specific reviews, considering budget, skills shortages and legacy systems.

Key Control Domains & Focus Areas

Core Cyber Security Control Domains to Audit

CIGFARO
Chartered Institute of
ment Finance, Audit & Risk Officers

Primary control families for government environments

I Identity

Strong authentication, privileged access control, joiner-mover-leaver discipline, and least-privilege design reduce unauthorized access.

N Network

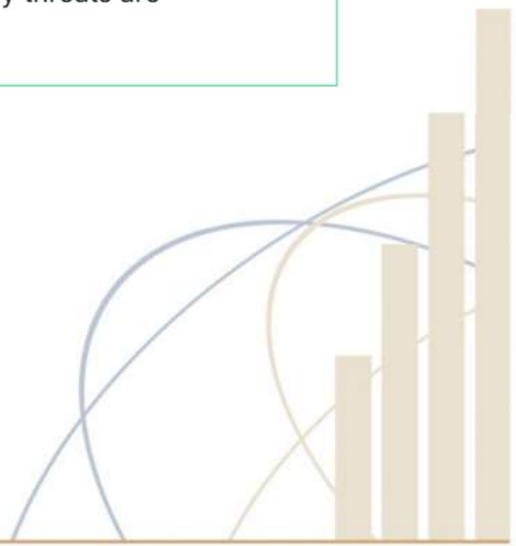
Segmentation, firewall governance, secure remote access, and hardened endpoints limit lateral movement and malware spread.

D Data

Encryption, backup integrity, retention controls, and recovery testing protect sensitive information and operational continuity.

M Monitoring

Central logging, alert triage, incident playbooks, and escalation paths determine how quickly threats are discovered and contained.



Threats, Vulnerabilities & Risk Prioritization

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

From attack vectors to impact-based ranking

Attack paths

Phishing, credential stuffing, exposed remote access, and malware delivery remain the most common entry points.

Legacy exposure

Unsupported operating systems, fragmented architectures, and unpatched devices increase the probability of compromise.

Internal and vendor risk

Privileged insiders, weak segregation of duties, and supplier access can amplify damage and bypass perimeter controls.

Impact ranking

Risks should be sorted by service criticality, data sensitivity, recovery difficulty, and potential public harm.

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Methodologies, Frameworks & Processes

Applicable Standards & Frameworks

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

International & Local Cybersecurity Standards

Apply ISO/IEC 27001/27002, ISO 22301, NIST CSF and COBIT, aligned with South African public sector guidance, including AGSA publications and National Treasury frameworks for minimum cybersecurity controls.

Sector Requirements, Mapping & Maturity Models

Incorporate sector-specific requirements for health, utilities, public safety and revenue collection, mapping frameworks to audit criteria, control objectives and maturity models to benchmark progress.

Audit Methodology, Evidence Collection & Testing Approach

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

How assurance is built from multiple evidence sources

Review

Policies, standards, architecture diagrams, risk registers, and prior reports establish the control baseline and context.

Sampling

Configuration samples and access reviews test whether controls operate consistently across representative systems and users.

Logs

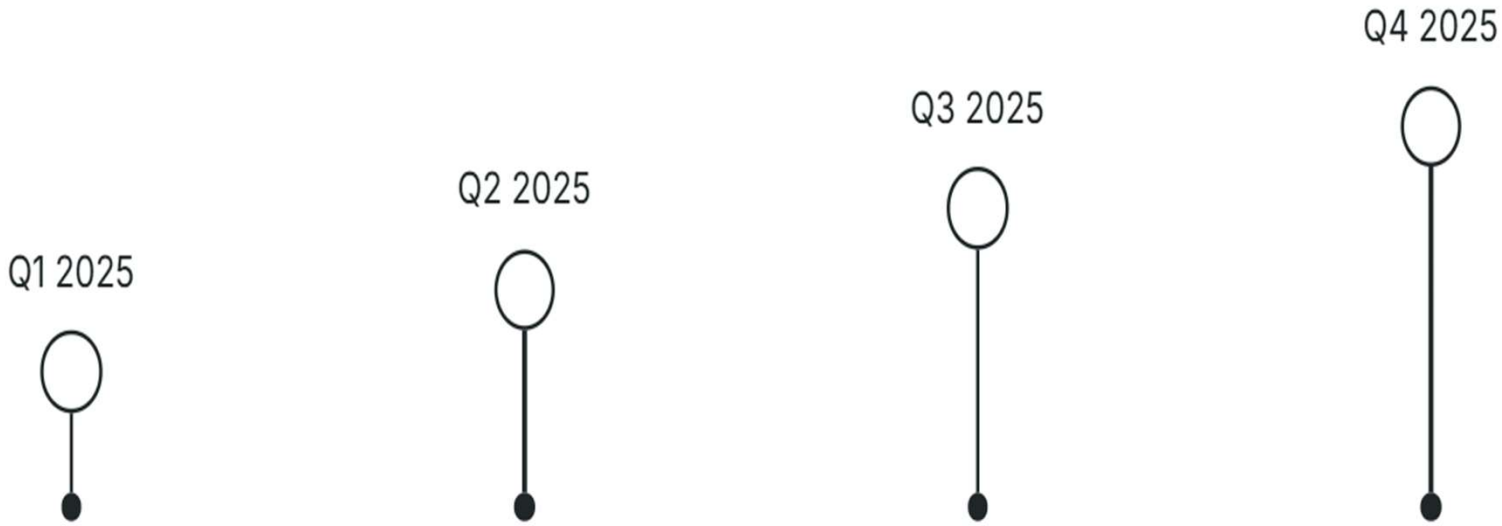
Event records, SIEM alerts, and incident tickets reveal detection quality, escalation speed, and control breakdown patterns.

Interviews

Walkthroughs with owners and operators validate how procedures work in practice, not only on paper.

Audit Methodology, Evidence Collection & Testing Approach

Turning audit results into sequenced corrective action



Diagnose

Identify control gaps
confirm root causes
validate scope
classify findings by risk and business impact.

Stabilize

Implement urgent fixes
address material weaknesses
reduce exposure in high-value systems and privileged accounts.

Embed

Standardize procedures
strengthen monitoring
assign owners
measure remediation progress through governance reporting.

Verify

Test management responses
confirm closure evidence
reassess residual risk
refresh the remediation backlog.

Audit Methodology, Evidence Collection & Testing Approach

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Building resilient, accountable, and secure government digital services

- **Audit lessons**: Security failures usually reflect weak governance, poor visibility, and inconsistent execution more than isolated technical flaws.
- **Governance**: Leadership must own risk decisions, resource remediation, and demand measurable accountability across all spheres of government.
- **Monitoring**: Continuous detection, periodic reassessment, and exception tracking are essential to sustain control effectiveness over time.
- **Next steps**: Prioritize high-risk controls, formalize ownership, and institutionalize repeat audits to improve assurance year by year.

Cyber Security Audit Lifecycle & Process

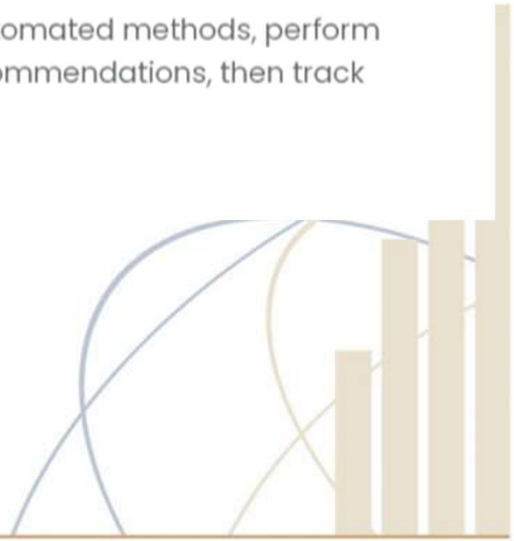
CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Audit Planning and Environment Analysis

Plan by assessing cyber risks, defining objectives, scope and resources, then map IT architecture, critical systems and data flows to understand dependencies, exposure points and control landscape.

Testing, Reporting and Remediation Flow

Test control design and effectiveness using manual and automated methods, perform technical assessments, report findings with ratings and recommendations, then track remediation actions and conduct targeted re-testing.



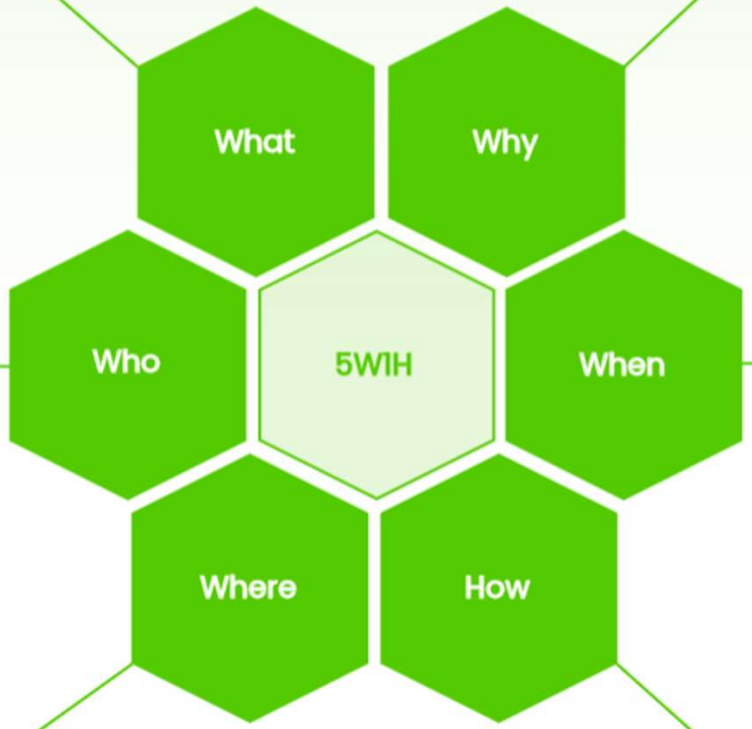
5W1H of Public Cyber Audits

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Public sector cyber audits assess security controls, governance processes and risk management across key domains, including access control, network security, incident response, data protection and compliance with legislation.

Audits cover national and local government departments, agencies and public entities, and are performed by internal audit teams, external specialist firms or co-sourced teams combining public sector and private expertise.

Audit work spans government on-premise data centers, regional and remote offices, cloud-based environments, shared service platforms and third-party hosting locations supporting critical public services.



Audits are driven by the need to protect citizen data, maintain essential service continuity, safeguard financial transactions, ensure compliance with laws and sustain public trust in government digital services.

Audits occur on regular cycles, such as annually or biannually, and may be triggered by major cyber incidents, significant system upgrades, migrations to cloud platforms or the introduction of new cybersecurity legislation.

Auditors use a mix of document review, stakeholder interviews, technical security testing, configuration analysis and data analytics to evaluate control effectiveness and identify gaps and improvement opportunities.

Question for the future of IT Systems risk and audit practices

Core methods and evidence sources

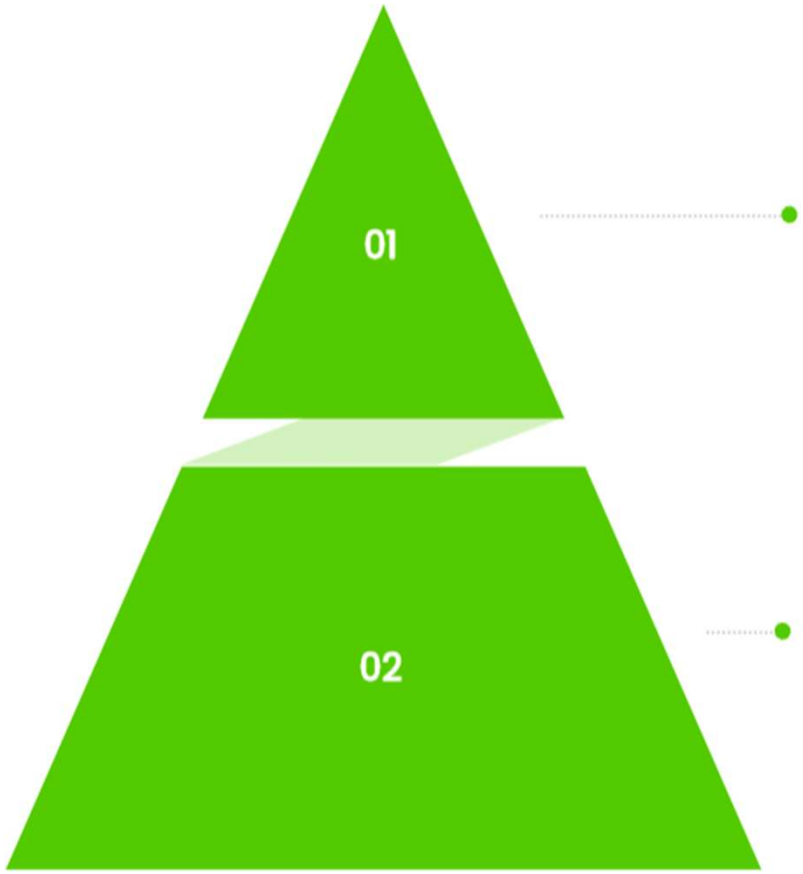
Apply automated tools for vulnerabilities, SIEM and configurations; select representative samples; gather policies, logs, tickets, change records, risk registers and contracts as primary audit evidence.

Analysis, handling and limitations management

Use data analytics to detect anomalies and control failures; ensure secure handling of sensitive evidence; address limitations from incomplete or legacy documentation through corroboration and professional judgment.

Governance, Control & Risk Management

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



Strategic Governance Layer

Define national-aligned cyber strategy, clear governance structures, and formalized roles and responsibilities to ensure accountable decision-making and effective oversight across government entities.

Policy, Risk and Operational Layer

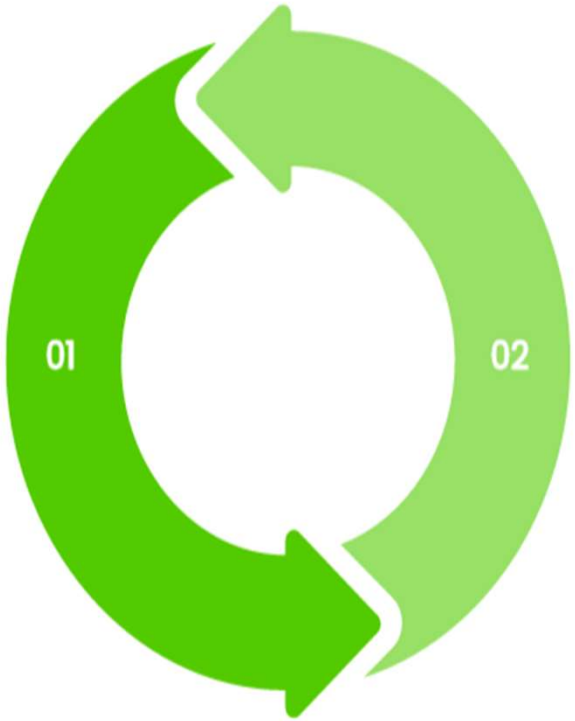
Enforce compliant policies, risk processes, third-party controls, continuous awareness, and performance reporting, ensuring cyber risks are systematically managed and transparently monitored.

Incident Response, Business Continuity & Resilience

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Preparation & Detection

Establish incident response plans, roles, contacts and playbooks. Enable timely detection, triage and classification of incidents and breaches using monitoring, alerts and clear escalation paths.



Response, Recovery & Continuous Improvement

Execute containment, eradication and recovery processes. Conduct post-incident reviews, update controls, align with business continuity and disaster recovery, and coordinate with regulators, law enforcement and stakeholders.

Data Protection, Privacy & Compliance

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

POPIA Compliance & Data Lifecycle Controls

Assess lawful processing, informed consent, purpose limitation, and data subject rights, including classification, retention schedules, secure destruction, and cross-departmental access within South African government entities.

Information Sharing, Legal Duties & Policy Alignment

Evaluate cross-border transfers, shared databases, records management, cybercrime reporting and evidence preservation, ensuring alignment with HR, procurement and disciplinary policies, and broader regulatory compliance.

Challenges, Gaps & Improvement Roadmap

Cyber Maturity Tiers

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Thinking	National	Provincial	Local
Past	Historically higher budgets and central mandates enabled basic cyber controls, but reliance on SITA and legacy systems created uneven maturity across national departments.	Provincial departments previously depended heavily on national guidance and SITA, with limited in-house skills and modest security budgets constrained by service delivery pressures.	Municipalities historically had very low cyber focus, minimal dedicated budgets, scarce skills and basic connectivity, with critical revenue and utility systems often poorly protected.
VS			
Now	Today national departments generally show the highest cyber maturity, with better skills, shared capabilities and formal governance, yet gaps remain in uniform implementation and rural-linked services.	Currently provinces exhibit mid-range maturity, with some own SOC or shared services, variable reliance on SITA, and uneven coverage between urban hubs and remote rural districts.	Today local governments show the lowest maturity, especially in rural areas, with patchy connectivity, ad hoc dependence on SITA or vendors, and high cyber risk to water, electricity and billing.
VS			
Future	In future national entities are expected to drive integrated security architecture, fund shared platforms and uplift lower spheres through standards, monitoring and centralized cyber support.	Going forward provinces aim to strengthen regional cyber hubs, enhance skills, coordinate municipalities, and better secure health, education and policing systems across mixed geographies.	In future municipalities need targeted funding, shared platforms and training to secure revenue, water, electricity and local policing services, reducing outage, fraud and service disruption risks.

Entity Action Plan

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Work Plan

Key work plan for the first half of the year
Jan. → Jun.

Key work plan for the second half of the year
Jul. → Dec.

Short-term Focus

Define and implement quick-win security controls to address high-risk gaps within 12 months, including patching, access reviews, and basic monitoring; prioritize remediation of critical vulnerabilities and high-risk findings identified in recent audits to rapidly reduce exposure.

Medium-term Focus

Over the next 1–3 years, strengthen cyber governance structures, clarify roles and accountability, and modernize core security architecture; align policies, standards, and reference architectures to enable consistent, risk-based decision-making across government entities.

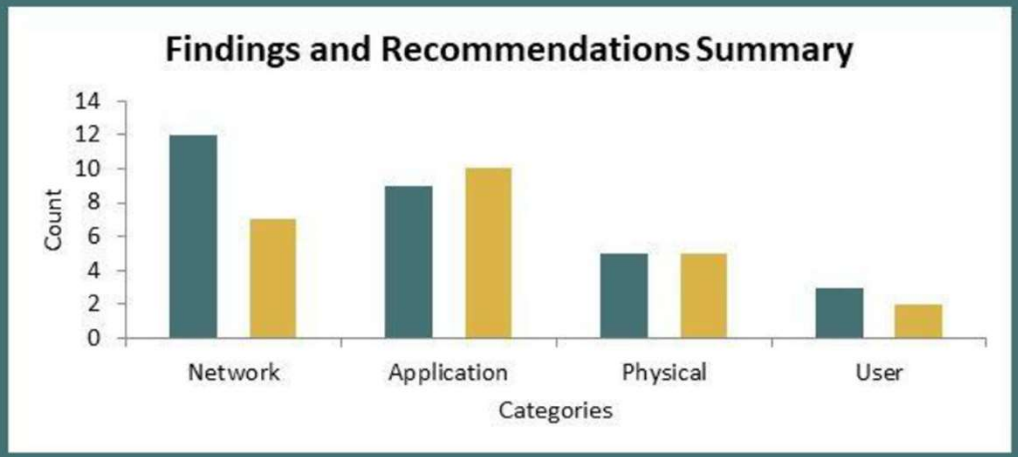
Long-term Focus

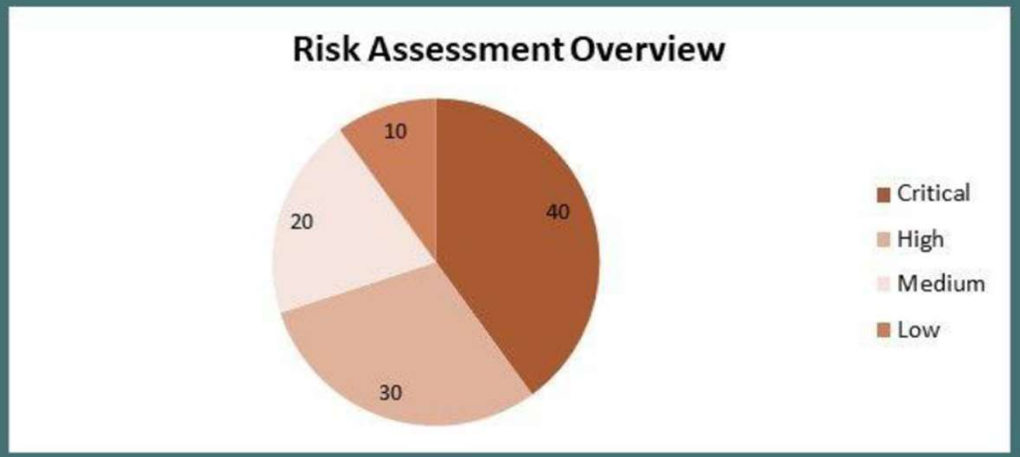
Within 3–5 years, establish integrated security operations that consolidate visibility, standardize incident response, and enable advanced monitoring and analytics; leverage shared platforms and automation to detect, investigate, and respond to threats at scale.

Capability & Collaboration

Build sustainable cyber capacity through targeted training, professional certifications, and formal communities of practice; enhance collaboration via inter-governmental cooperation, shared SOC arrangements, and coordinated sector-wide security initiatives.

Cracking Reporting of Cyber Security, Findings & Outcomes





Risk Level	Action Required	Audit Scope	Compliance Status
High ▲	Yes ▼	Limited ▲	Audit/Check ▼

Source: Future Spot

Conclusion & Recommendations:

Cybersecurity remains a primary concern. Cyber Security should be approached on the assumption that incidents would occur. ALL Spheres of Government are urged to put mechanisms in place to recover from potential cyber events, including continuous staff education.

- Organisational Cyber Awareness Campaigns
- 3rd Party Cyber Security Awareness & Governance
- Training & Development - with skills and capabilities developed to provide insight and recommendations

Recommendations:

- Organisations must run a 24-hour scan on the data centres to ensure data security
- Back – Ups are essential and should be consistent.
- Many organisations had been operating on legacy systems, and required substantial modernisation to strengthen its cybersecurity posture.
- A plan for IT investment over the next five years would address this challenge

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body