02 June 2026

Cyber Resilience Strategies

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Jonathan Kleinhans
Hessequa Municipality / ICT Manager

www.cigfaro.co.za

SAQA Recognised Professional Body

THE AUDIT MIRROR

What AGSA found

Combined MFMA 2023–24 and PFMA 2024–25 general reports

16%	64%	83%	R12.1bn
municipalities with clean audits (MFMA)	of reviewed entities: notable cybersecurity weaknesses (PFMA)	municipalities materially non-compliant with legislation (MFMA)	ICT projects with audit findings (PFMA)

11% of reviewed entities had critical vulnerabilities actively exploitable at the time of audit.
These are not projections. They are audited findings.

- *For public institutions, the issue is not only prevention — it is continuity of service, trust, and recovery speed.*

THE GOVERNANCE DIAGNOSIS

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Why the audit findings are not a technology problem

AGSA finding	What it means for ICT governance
Only 16% of municipalities achieved clean audits	Basic control environments — the foundation for any governance framework — are absent in 84% of institutions
ICT not viewed as a strategic enabler at metro level	If metros fail on this, the rest of local government has no floor to stand on
64% of national/provincial entities: notable cybersecurity weaknesses	Weakness is the norm, not the exception, across all spheres of government
Backup testing, incident response, and recovery procedures absent in majority of reviewed entities	The most basic cyber resilience requirements — not advanced tools — are missing
Vacancies in CRO, CAE, and CFO positions widespread	The governance roles that own risk are unfilled. No owner means no accountability.

The audit evidence does not describe a technology failure. It describes a governance failure with technology consequences.

THE STRATEGIC SHIFT

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

From cybersecurity to cyber resilience — and why it matters for government

Cybersecurity asks	Cyber resilience asks
How do we stop attacks?	How do we keep functioning when attacks succeed?
How do we build stronger walls?	How do we contain damage and recover rapidly?
Is our technology secure?	Can we continue delivering services during and after an incident?
Did we prevent the breach?	How quickly did we detect, respond, and recover?

The principle of assumed compromise

Operate on the assumption that the environment may already be compromised. Attackers may be inside. Vendors may be breached. Users will click malicious links. The strategic question is not whether disruption will occur — it is how quickly and effectively the institution can contain it and recover.

AGSA's penetration testing findings across national and provincial government confirm this is not a theoretical posture. It is the current reality.

The framework

HOW RESILIENCE IS BUILT

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Eight institutional pillars and the five NIST functions

The eight institutional pillars

1	**Governance** Accountability, policy, oversight, risk ownership	2	**People** Awareness, training, skills, role clarity
3	**Operations** Consistent controls, change management, vendor oversight	4	**Infrastructure** Reliable systems, power continuity, connectivity
5	**Security** Protection and detection controls proportionate to risk	6	**Continuity** Service recovery, BCP, disaster recovery
7	**Partnerships** Intergovernmental, shared services, support networks	8	**Adaptability** Continuous improvement, maturity progression

Technology sits inside pillar 5 (Security) only. Governance is the outer ring. Everything else enables it.

THE CAPACITY REALITY

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Resilience must be proportionate, honest, and tiered

No ICT capacity *Objective: survive and recover*	**Weak capacity** *Objective: contain and recover quickly*	**Well-capacitated** *Objective: operate through disruption*
Governance owner at Accounting Officer level Offline backup and tested restoration Documented incident contact list MFA on all user accounts Shared service or district ICT unit Manual fallback plan for critical services	**Above, plus:** Asset register and basic risk assessment ICT champion at senior management level Formal incident response procedure Annual BCP test Vendor contracts with clear SLAs	**Above, plus:** IT Strategy Committee and CIO function ISO 27001-aligned ISMS SOC or managed SIEM DR site with defined RTO and RPO Regular penetration testing

The governance obligation does not change with capacity. The response must be proportionate, but the accountability is constant.

THE SHARED SERVICE IMPERATIVE

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

For municipalities that cannot sustain independent cyber capability

The reality	The model
Many municipalities have zero dedicated ICT staff	District-level shared ICT units carry the governance and operational load
Independent cyber capability is not financially viable at local level	Provincial support hubs provide access to expertise, tools, and incident response
No single municipality can afford a SOC	Shared SOC services — accessible to all participating municipalities — are the only viable path
Vendor relationships are ungoverned	Shared procurement frameworks with standard SLAs reduce dependency and restore accountability
Intergovernmental support is slow to reach municipalities in distress	WCG has assisted 24 of 29 Western Cape municipalities — proof that structured support works

Shared services are not a workaround for weak municipalities. For the majority of South African local government, they are the only governance model that is honest about capacity.

THE QUESTION AO's MUST ANSWER

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Can you demonstrate, to an auditor or to the public, that you have taken reasonable and proportionate steps to govern your digital environment in relation to your risk exposure?

Three questions to ask in your institution today

1	What is your highest-risk system — and who is formally accountable for its security?
2	Who owns ICT risk in this institution — and does council receive regular cyber risk reporting?
3	If your billing system went down tonight — what is your recovery plan, and who executes it?

IMPORTANT:

You don't start with tools. You start with risk, mandate, and accountability.

AFTER INCIDENT: PRACTICE VS REALITY

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

A self-assessment for municipalities that have recently experienced a cyber incident

Area	What the framework requires	What typically existed at point of incident	Reflection question
Governance ownership	Named ICT risk owner at Accounting Officer level	ICT risk owned informally; no council resolution on cyber risk	*Who owned this risk before the incident?*
Asset visibility	Current register covering all systems, data, and third-party access	No asset register, or register outdated; vendor systems not inventoried	*Did we know what we had before it was compromised?*
Detection capability	Logging and alerting in place; tested escalation threshold	Incident discovered externally or by accident; no baseline for anomaly detection	*How long was the attacker inside before we knew?*
Incident response	Documented plan; defined roles; tested annually; legal and comms process clear	No plan; ad hoc response; vendor called without contract or SLA	*Did we respond to a plan — or improvise under pressure?*
Recovery capability	Tested backups; defined RTO and RPO; manual fallback for critical services	Backups untested or connected to compromised network; no RTO defined	*How long were services offline — and was that acceptable?*
Disclosure and learning	POPIA notification met; council informed; post-incident review conducted and acted on	Disclosure delayed; council not formally informed; no post-incident review documented	*Did we tell who needed to know — and did we learn?*

An incident is not a failure of technology. It is an audit of governance. The question now is whether the institution responds differently than it did before.

“Cyber resilience is a governance and service-delivery capability — not just an ICT control set.”

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body