Republic of Kenya

PUBLIC SECTOR ACCOUNTING STANDARDS BOARD (KENYA)

GOVERNMENT OF KENYA

DRAFT ICT GOVERNANCE AUDIT PROGRAMS FOR NATIONAL GOVERNMENT

SEPTEMBER 2026

ICT GOVERNANCE

(To be customised for each Program)

Audit Program No.:	**Period Under Review:**	**Department:**
Prepared By:		
Reviewed By:		

Audit Objective: To ascertain whether IT systems comply with applicable laws, regulations, contracts, industry guidelines, governance criteria, policies, and procedures.	
Risk: IT systems, data handling processes, or third-party service agreements do not align with the applicable laws, regulations, contracts , industry guidelines, governance criteria, policies, and procedures leading to Compliance Drift.	
Control	**Audit Tests**
An approved ICT policy is reviewed at least every 3 years.	**Test of Design** • Establish the key requirements of laws, regulations, policies and procedures in the development of ICT Policy • If the control is not documented, enquire from process owner how it is meant to be executed. **Test of Implementation** • Obtain the ICT Policy • Confirm that the design documented under TOD is implemented as documented. • Walkthrough and note any gaps in implementation

CPA Centre, 8th Floor, Thika Road, Ruaraka. P.O Box 38831 - 00100, Nairobi, Kenya. Tel: 020 251 1557
www.psasb.go.ke. email: info@psasb.go.ke

	Test of Operating Effectiveness • Confirm the existence of ICT Policy Section 11.5 of ICT Governance Standard 2023 • Confirm that the ICT Policy is in compliance with the National ICT roadmap and Vision 2030. (Vision 2030 & National ICT roadmap) • Confirm whether the ICT Policy has been approved by the governing body • Confirm whether the ICT Policy is aligned to applicable laws, regulations, and industry guidelines - *Applicable section of the laws, regulations and industry guidelines that is infringed.* • Confirm that the policy covers the following aspects. – Access Control (*section 11 of ICT security standard)* – Password Policy (*section 11.5.14 of ICT security standard)* – Child online safety policy (*section 11.9 of ICT security standard)* – Change Management policies and procedures (*section 11.13 of ICT security standard)* – Cryptographic policy (*section 12.1 of ICT security standard)* – Vendor Management Policy (*section 13.1.1.1 of ICT security standard)* – Policy on intellectual rights (*section 14. of ICT security standard)* – Data policy for privacy and protection of personally identifiable information (*section 14.4.1 of ICT security standard)* – Information Security policy (*section 11 of ICT security standard)* – Confidentiality policy (*section 7.3.10.2 of ICT security standard)* – Data Integrity policy (*section 7.3.10.4 of ICT security standard)* – Exit strategy policy (*section 7.3.10.6 of ICT security standard)* – Information transfer policy (*section 8.2 of ICT security standard)* – Electronic messaging policy (*section 8.3 of ICT security standard)* – Clear desk and clear screen policy (*section 9.1.4&5 of ICT security standard)* – Back up policy (*section 9.3.1.1 of ICT security standard)*

	– Incident management policy (*section 9.4.8 of ICT security standard)* – User end-point device security policy (*section 10 of ICT security standard)* – Remote working policy (*section 10.1.3 of ICT security standard)* – ICT training policy (*section 14.6 of ICT Governance standard)* – ICT enterprise security architecture policy and procedures (security architecture principle 6 of governing principles) – Electronic records management policy (section 7.1.2 of the electronic records management standard) – Bring your own device policy (section 8.4 of the end user computing standard) – Acceptable internet usage policy (section 8.6 of govt ICT networks) – Policy on governance of information assets (Annex A.10 on ICT human capital and development standard) – Policy on information security testing. (Annex A.10 on ICT human capital and development standard) • Carry out other tests for operating effectiveness aligned to specific entity policies, procedures, service delivery standards, minutes of meetings. • Obtain and Review the ICT Policy. Does it address emerging risks (AI, Cyber) and align with ICTA standards?
Audit Objective: To confirm if the ICT strategy is documented, approved, and aligned with the entity's goals and Kenya's National ICT Roadmap.	
Risk: ICT initiatives do not support entity or Government (Vision 2030) objectives.	
Control	**Audit Tests**
An approved ICT Strategic Plan	**Test of Design**

is reviewed regularly	• Establish the key requirements of laws, regulations, policies and procedures in the development of ICT strategy. • If the control is not documented, enquire from the process owner how it is meant to be executed. **Test of Implementation** • Obtaining ICT strategy • Confirm that the design documented under TOD is implemented as documented. • Walkthrough and note any gaps in implementation **Test of Operating Effectiveness** • Confirm the existence of ICT strategy Section 14.4 of ICT Governance Standard 2023 • Examine relevant committees minutes to confirm the strategy was formally reviewed and approved. • Carry out other tests for operating effectiveness aligned to specific entity policies, procedures, service delivery standards, minutes of meetings, and strategic plans. • Review the ICT Strategic Plan. Establish if the entity has an ICT Strategic Plan covering the current period (e.g., 2023–2027). Ascertain if it addresses emerging risks (AI, Cyber) and aligns with ICTA standards? • Obtain the entity's Strategic Plan and compare it against the ICT Strategic Plan. Look for mapped dependencies and note the gaps. • Interview department heads to establish if the ICT strategy addresses their specific operational pain points. • Inspect the strategy for a clear roadmap on Cloud vs. On-Premise infrastructure. Does it account for future data growth? • Identify "End-of-Life" (EOL) systems. Check if the strategy includes a funded decommissioning or replacement plan for these risks.

	• Review the list of approved technologies to ensure the environment isn't becoming overly complex with redundant tools. • Ascertain if the strategy accounts for the "People" factor, or is it just focused on "Gear-IT aspects only"? • Review the current IT org chart against the strategic goals (e.g., if the strategy is "AI-First," does the team actually have Data Scientists?). • Verify that a training budget exists and is being used specifically for certifications aligned with the new strategy. • Confirm that risks identified in the ICT Strategy are also reflected in the Enterprise Risk Register. • Review the New Projects in the pipeline to ensure a Security Impact Assessment is a mandatory step in the planning phase. • Check if the ICT strategy includes updates to DR capabilities as new technologies are introduced
Audit Objective: To verify that there is an authorized ICT Governance structure.	
Risk: lack of oversight for ICT investments and Strategic Misalignment	
Control	**Audit Tests**
ICT Governance committees with formal Terms of Reference (ToR) established.	**Test of Design** • Establish the key requirements of laws, regulations, policies, and procedures in the establishment of ICT Governance committees. • If the control is not documented, enquire from process owner how it is meant to be executed. **Test of Implementation** • Obtain appointment letter of the committee member. • Confirm that the design documented under TOD is implemented as documented. • Walkthrough and note any gaps in implementation

	Test of Operating Effectiveness • Confirm the existence of ICT governance committees (e.g., ICT Strategy Committee, IT Steering Committee) Section 9.2 of ICT Governance Standard 2023, Appendix 1 *of ICT Governance Standard 2023.* • Obtain the terms of reference for the committee members and confirm that the terms are aligned to the responsibilities set out in Appendix 1 *of ICT Governance Standard 2023.* • Review of ICT strategy committee minutes, reports and correspondence to confirm that it undertakes the following duties: *a.* Provides *insight and advice to the board on topics such as:* *-The relevance of the development in IT from a business perspective* *-The alignment of IT with the business direction* *-The achievement of strategic IT objectives* *-The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives* *-Optimization of IT costs, including the role of and value delivery of external IT sourcing* *-Risk, return and competitive aspects of IT investments* *-The contribution of IT to the business.* *-Exposure to IT Risks, including compliance risks* *-Direction to management relative to IT strategy* *-Drivers and catalysts for the boards IT* b. Review ICT steering committee minutes, reports and correspondences to confirm that it undertakes the following duties: *-Decides the overall level of IT spending and how costs will be allocated* *-Aligns and approves the enterprise's IT architecture* *-Approves project plans and budgets, setting priorities and milestones*

	-Acquires and assigns appropriate resources *-Ensures that projects continuously meet business requirements including a reevaluation of the business case* *-Monitors projects plan for delivery of expected value and desired outcomes, on time and within budget* *-Monitors resource and priority conflict between enterprise divisions and the IT functions as well as between projects.* *-Makes recommendations and requests for changes to strategic plans (Priorities, funding, technology approaches and resources)* *-Communicates strategic goals to projects teams* *-It is a major contributor to management's IT governance responsibilities and practices* • Carry out other tests for operating effectiveness aligned to specific entity policies, procedures, service delivery standards, minutes of meetings and strategic plans. • Obtain and review ICT Steering Committee minutes for the last 12 months. • Verify they meet at least quarterly, and evidence of active challenge of ICT performance.
Audit Objective: To verify that IT spending is in line with strategy.	
Risk: Sub-optimal IT Investment and Resource Wastage	
Control	**Audit Tests**
Formal Project Appraisal and Post-Implementation Review	**Test of Design** • Establish the key requirements for the Business Case/ Feasibility Study or Post-Implementation Review • If the control is not documented, enquire from process owner how it is meant to be executed. **Test of Implementation**

	• Select one Information System asset • Confirm that the design documented under TOD is implemented as documented. • Walkthrough and document the process flow/ map. Note any gaps in implementation **Test of Operating Effectiveness** • Confirm that policies are carried out efficiently and wastage of public funds is eliminated (Value for money) *PFM Reg. 43(d) of 2015.* Check for; ✓ Unused information assets ✓ Overpriced assets • Analyze the variance between the ICT budget and actual spend. Investigate any unapproved overruns • Sample major IT projects as per the approved entity sampling criteria and confirm whether the Expected Benefits defined in the business case were actually measured and achieved.