Based on the Council Law of 2004, Article (5), Paragraph (2), which stipulates that the Council may establish internal regulations to govern its work, the Council has issued these regulations governing digital transformation activities.

Digital Transformation Framework

1. Purpose

This Digital Transformation Framework establishes the principles, priorities, governance arrangements, and implementation directions for the Council's digital modernization in support of regulatory effectiveness, operational efficiency, stakeholder service, data integrity, and institutional resilience.

2. Strategic Aim

The Council shall transform its core services, records, workflows, examinations, communication, and oversight capabilities through secure, reliable, and user-centered digital systems.

3. Guiding Principles

Digital transformation shall be guided by legality, security, service quality, accessibility, transparency, accuracy, interoperability, accountability, sustainability, protection of confidential and sensitive information, and resilience against cyber and operational disruption. The Council should draw on ICT and digital transformation guidance developed for professional accountancy organizations in Africa and broader international digital governance practice.

4. Objectives

The Council's digital transformation objectives shall include digitizing registration and licensing, modernizing examination administration, strengthening records management, enabling data-driven oversight, improving stakeholder communication, enhancing cybersecurity, and supporting efficient internal administration.

5. Priority Digital Domains

Registration and Licensing: online applications, document upload, fee processing, renewal workflows, status tracking, and digital registers.

Examinations: candidate portals, scheduling, digital communications, results publication, incident logging, examiner coordination, and where feasible secure computer-based assessment.

Records and Archives: secure digital repositories for Board decisions, committee records, standards, registrations, disciplinary files, and institutional documents.

Finance and Administration: digital budgeting, approvals, procurement support, HR workflows, and management reporting.

Stakeholder Engagement: official website services, notices, candidate information, registrant communication, helpdesk functions, and public access to appropriate information.

Analytics and Oversight: dashboards, performance reports, compliance tracking, examination statistics, and risk monitoring.

6. Digital Governance

The Board shall oversee digital transformation through the Information Technology and Digital Transformation Committee, with management responsible for execution, controls, procurement planning, user support, and reporting.

7. Data Governance

The Council shall maintain clear rules for data ownership, classification, access rights, retention, backup, recovery, quality control, and authorized use. Sensitive personal, academic, regulatory, and disciplinary data shall receive enhanced protection.

8. Cybersecurity and Information Protection

The Council shall implement appropriate cybersecurity controls including user authentication, access management, secure storage, backup procedures, incident response, logging, system updates, and awareness measures for staff and users.

9. Digital Service Design

Digital services shall be designed to be practical, understandable, efficient, and accessible to users. User journeys should minimize duplication, reduce manual handling, and improve transparency of status and requirements.

10. System Procurement and Development

Technology solutions shall be selected or developed through structured planning that considers legal compliance, security, functionality, scalability, maintenance, cost-effectiveness, and vendor reliability.

11. Change Management and Capacity Building

Digital transformation shall be supported by staff training, stakeholder orientation, revised procedures, phased implementation, and communication plans to encourage adoption and reduce operational disruption.

12. Business Continuity

Critical digital systems shall be supported by backup, recovery, continuity planning, and fallback procedures to ensure resilience during outages, incidents, or emergencies.

13. Performance Measurement

The Council shall monitor digital transformation through indicators such as service uptake, processing time reductions, user satisfaction, system availability, data quality, security incident trends, and efficiency gains.

14. Phased Implementation

Implementation should proceed in phases, beginning with high-impact services such as registration, examination administration, records digitization, and official communications, followed by analytics, workflow automation, and broader system integration.

15. Compliance and Review

All digital transformation activities shall comply with applicable law, Council regulations, approved policies, and data protection and confidentiality obligations. This Framework shall be reviewed periodically to reflect changes in technology, risk, and institutional priorities.

It was approved by circler.

Dr. Mohamed Hassan Azrag

AAPOC

President