QUALITY MANUAL

ICTA-DPS-QM-001

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

REVISION HISTORY

Revision/Version	Date of change	Description of Change	Approver details

ICT AUTHORITY (ICTA)

Head Office: P.O. Box 27150, Nairobi-00100, Tel.: (+254 202) 211 960/61
E-Mail: standards@ict.go.ke, Web: http://standards.icta.go.ke

DOCUMENT CONTROL

Document Name:	Quality Manual
Prepared by:	Deputy Director Standards and Processes
Edition:	First Edition
Approved by:	Director Programmes and Standards
Date Approved:	1st March 2025
Effective Date:	1st March 2025

CONTENTS

1.0 INTRODUCTION

1.1. Overview

The key mandate of the Information and Communication Technology Authority, as spelt out in the Legal Notice 183 of 2013, is to formulate, maintain and enforce ICT Standards that covers end to end ICT investment processes, across government agencies and ministries. In an endeavour to achieve this mandate, the Authority developed a framework of ICT standards for conceptualization, acquisition, operation and management and disposition of outdated, obsolete, faulty and expired ICT assets in Ministries Counties Departments Agencies. This framework of standards was formulated and developed based on the broadly acknowledged and globally accepted Government Enterprise Architecture (GEA) founded on the Open Group Standard's TOGAF.

1.2. Scope

Covers the development, administration, and maintenance of certification schemes for ICT professionals in the public service.

2.0 ROLES AND RESPONSIBILITIES

Assigned Role/Committee	Key Responsibilities
Quality Manager	Draft, review, and approve policies governing certification processes.
Deputy Director Standards	Ensure staff/assessors adhere to policies; monitor compliance.
Finance Department	Budgeting, financial reporting, and managing reserves/insurance.
HR and Administration, ICT, Planning and Research Divisions	Assign personnel, technology, and funds to certification activities.
Standards Development Department	Design, update, and maintain certification scheme.
Accreditation and Certification Department	Oversee assessor training, and assessment.
	Review assessment results; approve/reject certifications and scope changes.
Procurement Department	Negotiate and manage agreements with external partners.

3.0 DEFINITIONS

Term	Definition
Appeal	A request by an applicant or certificate holder for reconsideration of a decision made by the certification body (e.g., denial or withdrawal of certification).
Applicant	An individual seeking certification from the organization.
Certification Scheme	A structured framework defining the requirements, processes, and criteria for certifying individuals in a specific field
Competence	Demonstrated ability to apply knowledge, skills, and behaviours to perform tasks to the required standard as defined by ICTA's certification schemes.
Complaint	An expression of dissatisfaction by any party related to the certification body's activities, excluding appeals.
Evaluation	The process of determining an applicant's competence through methods such as examinations, interviews, practical assessments, or portfolio reviews.
ICT Authority	the entity responsible for developing, administering, and maintaining personnel certification schemes in compliance with ISO/IEC 17024.
Impartiality	The absence of bias or conflict of interest in certification activities, ensuring objectivity and fairness.
Nonconformity	A deviation from specified requirements (e.g., standards, procedures, or certification criteria).
Outsourcing	Use of external parties to perform activities on behalf of the certification body (e.g., exam administration, evaluation).
Surveillance	Ongoing monitoring of certified persons to ensure continued compliance with certification requirements.

4.0 GENERAL REQUIREMENTS

4.1. Legal entity

The ICT Authority is a governmental body created under legal notice 183 of August 2013. It's mandated to accredit ICT professionals and operating the certification scheme in line with Government ICT standards.

4.2. Responsibility for decision on certification

The ICT Authority shall retain authority over all certification decisions, including granting, maintaining, suspending, and withdrawing certification. These decisions shall be made by the Authority based on objective evidence and compliance with predefined criteria.

4.3. Management of impartiality

4.3.1 The ICT Authority has documented its structure, policies and procedures to manage impartiality and to ensure that the certification activities are undertaken impartially. The ICT Authority has appointed an impartiality committee that is the mechanism for ensuring impartiality.
The ICT Authority top management has published the Public Impartiality Statement on the ICT Authority's website homepage, certification application forms, and official communications.

4.3.2 The ICT Authority shall act impartially in relation to its applicants, candidates and certified persons.

4.3.3 The ICT Authority has documented policies (ICTA/DPS/Pol/YY) and procedures (ICTA-DPS-XXX-001) designed to ensure fairness, equal opportunity and consistent treatment for all applicants, candidates, and certified professionals, regardless of background, affiliation, or status.

4.3.4 The ICT Authority shall ensure that certification eligibility and access is based solely on merit and competency, not be restricted on the grounds of undue financial or other limiting conditions, such as membership of an association or group. Procedures shall be designed to minimize barriers and ensure equitable opportunities for all candidates.

4.3.5 The ICT Authority shall ensure the impartiality of its certification activities and shall not allow commercial, financial or other pressures to compromise impartiality.

4.3.6 The ICT Authority shall identify threats to its impartiality on an ongoing basis. This includes threats arising from its operations, affiliated entities, organizational relationships, or from the relationships of its personnel. However, the existence of such relationships does not inherently constitute a threat to impartiality.

4.3.7 The ICT Authority shall assess, document, and mitigate potential conflicts of interest arising from its certification activities. The Authority shall maintain documentation and demonstrate how it eliminates, minimizes, or manages such threats. This includes all identified potential sources of conflict, whether internal (e.g., personnel responsibilities) or external (e.g., third-party entities, partners, or affiliated organizations)."

4.3.8 The ICT Authority shall structure and manage its certification activities to safeguard impartiality. This includes ensuring balanced involvement of interested parties in all relevant processes.

4.4. Finance and liability

The ICT Authority shall maintain a detailed financial plan, including annual budgets and revenue streams from certification fees. The ICT Authority shall hold indemnity insurance to address claims arising from certification decisions, errors, or omissions. Policy details shall be reviewed annually for adequacy.

5.0 STRUCTURAL REQUIREMENTS

5.1. Management and organization structure

5.1.1 The ICT Authority shall ensure impartiality is embedded in the design and execution of all certification activities. Organizational structures, workflows, and management practices shall be systematically aligned to eliminate bias and uphold objectivity. Appendix I

5.1.2 The ICT Authority shall operate as a semi-autonomous government agency under the Ministry of Information, Communications and the Digital Economy (MICDE), with delegated authority to manage certification activities independently. Reporting lines and interactions with the Ministry are defined in Appendix II

5.2. Structure of the certification body in relation to training

5.2.1 The ICT Authority shall permit training as part of certification schemes to enhance candidate preparedness. However, the approval of training programs is strictly impartial, and certification assessments remain independent of training providers. Compliance with competency standards is non-negotiable, regardless of training participation.

5.2.2 The ICT Authority shall provide transparent information about education and training prerequisites required for certification eligibility. However, the Authority shall avoid endorsing or promoting specific training providers and ensures no claims are made that suggest preferential treatment or reduced rigor for candidates using such services.

5.2.3 The ICT Authority acknowledges the inherent risks to impartiality when offering training and certification under the same legal entity. To mitigate these risks, the Authority shall implement structural, procedural, and governance safeguards to ensure certification processes remain independent, fair, and free from undue influence. The ICT Authority shall ensure:

a) The impartiality committee conducts bi-annual reviews to identify threats. Findings are documented in the impartiality Risk Register, with mitigation plans approved by top management.
b) Certification and training teams operate in Accreditation and certification, and capacity development departments respectively with distinct reporting lines.
c) ensure that offering both training and certification services does not create any perception that utilizing both will result in a preferential advantage for the applicant.
d) not insist that candidates exclusively complete its own education or training programs when alternative programs offering equivalent outcomes are available.
e) ensure that any personnel who have provided training to a candidate are precluded from serving as that candidate's examiner for two years following the completion of the training. This period may be reduced if the Authority can demonstrate that a shorter interval would not compromise impartiality.

6.0 RESOURCE REQUIREMENTS

6.1. General personnel requirements

6.1.1 The ICT Authority shall assume accountability for the performance and conduct of all individuals engaged in certification processes. This includes ensuring personnel act impartially, maintain confidentiality, and possess the necessary competencies to fulfil their roles

6.1.2 The ICT Authority shall maintain an adequate pool of qualified personnel, ensuring that their expertise and capacity align with the scope, diversity, and volume of certification activities.

6.1.3 The ICT Authority shall establish clear competence criteria for all personnel involved in the certification process. Each individual must possess the necessary skills and expertise to effectively fulfil their assigned tasks and responsibilities.

6.1.4 The ICT Authority shall issue documented guidelines to all personnel, clearly outlining their duties and responsibilities. These guidelines must be reviewed and updated regularly to ensure they remain current.

6.1.5 The ICT Authority shall maintain comprehensive and current records for all personnel. These records must include pertinent details such as qualifications, training history, work experience, professional affiliations, current professional status, competence, and any known conflicts of interest.

6.1.6 The ICT Authority shall require that all personnel acting on its behalf maintain strict confidentiality regarding any information obtained or generated during certification activities. Disclosure is permitted only when mandated by law or explicitly authorized by the applicant, candidate, or certified individual.

6.1.7 The ICT Authority shall mandate that all personnel sign a formal commitment to comply with its established policies, including those governing confidentiality, impartiality, and conflict of interest.

6.1.8 The ICT Authority shall implement specific procedures to safeguard impartiality when certifying any of its own employees, ensuring that internal employment relationships do not compromise the fairness and objectivity of the certification process.

6.2. Personnel involved in the certification activities

6.2.1 General

The ICT Authority shall mandate that all personnel disclose any potential conflicts of interest related to any candidate.

6.2.2 Requirements for examiners

6.2.2.1 The ICT Authority shall ensure examiners are rigorously selected, trained, and approved to uphold the integrity of certification assessments. The examiners shall meet the following requirements:

a) Demonstrate a thorough understanding of the applicable certification scheme.

b) Capable of effectively applying the examination procedures and utilizing the associated documentation during the certification process.

c) possess the requisite expertise in the specific field under evaluation.

d) demonstrate fluency in both written and spoken forms of the examination language. When an interpreter or translator is utilized, the ICT Authority shall enforce procedures to ensure that the examination's validity remains uncompromised.

e) disclose any known conflicts of interest to ensure that all judgments remain impartial.

6.2.3.2 If any personnel involved in the assessment process exhibit a potential conflict of interest regarding a candidate, the ICT Authority shall implement procedures to protect the confidentiality and impartiality of the examination. All such procedures must be formally documented.

6.3. Outsourcing

6.3.1 The ICT Authority shall enter into legally binding agreements with every external organization involved in any outsourced work related to the certification process. These agreements must clearly address arrangements concerning confidentiality and the management of conflicts of interest.

6.3.2 When the ICT Authority outsources work related to certification, it shall:

a) assume ultimate responsibility for all certification processes, even when tasks are outsourced to external providers.
b) verify that any external entity performing outsourced work is fully qualified and consistently meets the relevant requirements of the ISO/IEC 17024 Standard.
c) regularly assess and monitor the performance of external organizations performing outsourced work, in strict accordance with its documented procedures.
d) maintain comprehensive records to confirm that external entities performing outsourced work fully meet all relevant requirements.
e) maintain an up-to-date list of all external organizations engaged in outsourced work.

6.4. Other resources

The ICT Authority shall ensure that all facilities—including examination sites, equipment, and other necessary resources—are appropriate and sufficient to support the effective delivery of its certification services.

7.0 RECORDS AND INFORMATION REQUIREMENTS

7.1 Records of applicants, candidates and certified persons

7.1.1 The ICT Authority shall maintain comprehensive, secure, and accessible records that verify the status of each certified individual. These records shall clearly demonstrate that the certification or recertification process has been properly executed. They shall include, but are not limited to, application forms, assessment reports (incorporating examination records), and other relevant documentation covering the granting, maintaining, recertifying, expanding or reducing the scope, and suspending or withdrawing of certification.

7.1.2 The ICT Authority shall ensure records are securely managed throughout their lifecycle, from creation to disposal. Retention periods shall align with legal, contractual, and operational requirements, while maintaining the confidentiality and integrity of all data

7.1.3 The ICT Authority shall establish enforceable agreements requiring certified professionals to promptly notify the Authority of any changes in circumstances that may affect their ability to meet certification requirements. This includes, but is not limited to, changes in employment, legal issues, loss of qualifications, or other factors impacting competency or ethical standing.

7.2 Public information

7.2.1 The ICT Authority shall verify and, upon request, provide confirmation of an individual's current and valid certification status, including the scope of that certification, unless prohibited by law.

7.2.2 The ICT Authority shall publish details on the scope of its certification scheme along with a general overview of the certification process, ensuring this information is readily accessible to the public without the need for a formal request.

7.2.3 The ICT Authority shall compile a complete list of all prerequisites for the certification scheme and make this list readily accessible to the public without requiring a formal request.

7.2.4 The ICT Authority shall ensure that all information disseminated, including advertising materials, is accurate and free from any misleading content.

7.3 Confidentiality

7.3.1 The ICT Authority shall establish comprehensive, documented policies and procedures governing the maintenance and controlled release of information.

7.3.2 The ICT Authority shall ensure, through legally binding agreements, that all information obtained during the certification process remains confidential. These agreements shall be extended to all personnel involved.

7.3.3 The ICT Authority shall ensure that any information obtained during the certification process—or from sources other than the applicant, candidate, or certified person—is not disclosed to unauthorized parties without the individual's explicit written consent, unless disclosure is mandated by law.

7.3.4 When the ICT Authority is legally obligated to disclose confidential information, it shall, unless prohibited by law, notify the individual concerned of the specific details that will be released.

7.3.5 The ICT Authority shall implement measures to ensure that the actions and operations of any related bodies do not compromise the confidentiality of information.

7.4 Security

7.4.1 The ICT Authority shall establish comprehensive, documented policies and procedures to secure every stage of the certification process. In addition, it shall implement robust mechanisms to promptly detect and address any security breaches, ensuring that corrective actions are taken as necessary.

7.4.2 The ICT Authority's security policies and procedures shall include specific measures designed to safeguard examination materials. These measures should address the following aspects:

a) the locations of the materials (e.g. transportation, electronic delivery, disposal, storage, examination centre);
b) the nature of the materials (e.g. electronic, paper, test equipment);
c) the steps in the examination process (e.g. development, administration, results reporting);
d) the threats arising from repeated use of examination materials.

7.4.3 The ICT Authority shall proactively implement measures to prevent any fraudulent practices during examinations by:

a) requiring candidates to sign a non-disclosure agreement—or an equivalent document—that obligates them not to divulge confidential examination materials and to refrain from any fraudulent test-taking practices.
b) requiring the presence of an invigilator or examiner during examinations to ensure that the process remains secure and free from fraudulent practices.
c) verifying the candidate's identity through established and reliable methods.
d) Establish and implementing procedures to ensure that no unauthorized aids are introduced into the examination area.

e) implementing measures to ensure that candidates are unable to access any unauthorized aids during the examination.
f) continuously review examination outcomes to detect any potential signs of cheating.

8.0 CERTIFICATION SCHEMES

8.1 The ICT Authority has established and maintains a certification schemes (put unique number) for each professional category it certifies.

8.2 The certification scheme encompasses the following components:
a) A clearly defined scope of certification.
b) Detailed job and task descriptions.
c) Clearly specified competence requirements.
d) Relevant abilities, where applicable.
e) Necessary prerequisites, where applicable.
f) A code of conduct, where applicable.

8.3 The certification scheme has incorporated the following process requirements:
a) Criteria for both initial certification and recertification.
b) Assessment methods to evaluate candidates for initial certification and recertification.
c) Surveillance methods and criteria, where applicable.
d) Criteria for suspending or withdrawing certification.
e) Criteria for modifying the scope or level of certification, where applicable.

8.4 The ICT Authority shall maintain documented evidence demonstrating that the development and periodic review of the certification scheme include:
a) The active involvement of suitably qualified experts.
b) The implementation of a balanced structure that equitably represents the interests of all significantly concerned parties, ensuring no single interest dominates.
c) The clear identification and alignment of any applicable prerequisites with the established competence requirements.
d) The determination and alignment of the assessment mechanisms to correspond with the competence requirements.
e) The regular conduct and updating of a job or practice analysis to ensure that current industry requirements are accurately reflected to:

- Identify the key tasks essential for effective performance.
- Define the specific competence required for each task.
- Determine any prerequisites that may apply.
- Confirm the appropriate assessment methods and the content of examinations.
- Specify the recertification requirements along with the corresponding interval.

8.5 The ICT Authority shall implement procedures to conduct regular, systematic reviews and validations of the certification scheme, ensuring its ongoing relevance, accuracy, and effectiveness.
8.6 When the ICT Authority is not the owner of the certification scheme it implements, it shall still ensure that all requirements outlined in Clause 8 are fully met.

9.0 CERTIFICATION PROCESS REQUIREMENTS

9.1 Application process

9.1.1 Upon application, the ICT Authority shall provide applicants with a clear and comprehensive overview of the certification process, aligned with the relevant certification scheme. At minimum, this overview shall include:

a) Certification Requirements: Eligibility criteria (e.g., education, experience, prerequisites).
b) Scope of Certification: Defined competencies and professional boundaries covered by the certification.
c) Assessment Process: Detailed steps (e.g., exams, practical evaluations, interviews) and timelines.
d) Applicant Rights: Rights to appeal decisions, access records, and submit complaints.
e) Certified Person Obligations: Duties such as maintaining competence, disclosing changes, and adhering to ethical standards.
f) Fee Structure: Transparent breakdown of costs (e.g., application, assessment, recertification).

9.1.2 The ICT Authority shall ensure that all applicants complete a standardized, signed application form that captures essential information, confirms compliance with certification requirements. The application form shall include the following mandatory sections:

a) Applicant Identification - Full name, contact details (address, email, phone), professional credentials (e.g., license number).
b) Scope of Certification - Specific certification sought (e.g., "ICT Technician"), including specializations.
c) Compliance Agreement - Signature/checkbox affirming: Agreement to comply with certification rules, Commitment to provide required documentation.
d) Supporting Documentation - List of prerequisites (e.g., transcripts, work experience proof) with upload instructions.
e) Special Needs Notice - Clear statement: "Applicants may request reasonable accommodations for disabilities or special needs (e.g., extra exam time, accessible formats). Contact [email/phone] to discuss."

9.1.3 The ICT Authority shall systematically review all applications to verify compliance with the eligibility criteria, documentation requirements, and scope defined in the relevant certification scheme.

9.2 Assessment process

9.2.1 The ICT Authority shall implement the assessment methods and mechanisms specified in each certification scheme to ensure evaluations are consistent, impartial, and aligned with the competencies defined for the certification category.

9.2.2 The ICT Authority commits to transparently documenting and communicating changes to certification schemes that require additional assessments. All updates to certification requirements, along with the corresponding assessment methods, will be made publicly accessible to ensure certified persons and applicants understand how to comply with revised standards.

9.2.3 The ICT Authority shall design and organize assessments to objectively and systematically verify that candidates meet all scheme requirements, using documented evidence to confirm their competence.

9.2.4 The ICT Authority shall review and confirm the effectiveness of all candidate assessment methods, ensuring that each assessment is conducted in a fair and valid manner.

9.2.5 The ICT Authority shall ensure fair and inclusive assessments by accommodating candidates with special needs while maintaining assessment integrity and complying with national regulations.

9.2.6 The ICT Authority shall ensure that any work performed by external bodies (e.g., assessments, training, evaluations) aligns with its certification scheme requirements. The Authority shall maintain documented evidence including reports, data and records to demonstrate equivalence and compliance with the requirements established by the certification scheme.

9.3 Examination process

9.3.1 The ICT Authority shall design examinations to objectively and reliably assess candidate competence in alignment with certification schemes. The design of examinations shall meet the following requirements:

a) Alignment with Certification Scheme: Ensure exams directly test competencies defined in the scheme.
b) Diverse Assessment Methods: Use written, oral, practical, and observational tools.
c) Consistency and Comparability: Standardize exams across administrations.
d) Valid Pass/Fail Decisions: Establish objective, competency-based criteria.

9.3.2 The ICT Authority shall establish documented procedures to guarantee that examinations are administered in a consistent manner, ensuring uniformity, fairness, and reliability throughout the process.

9.3.3 The ICT Authority shall define and document clear criteria for the conditions under which examinations are administered, and these criteria shall be regularly monitored to ensure ongoing compliance and consistency.

9.3.4 The ICT Authority shall ensure the accuracy, reliability, and consistency of all tools and systems involved in the assessment process.

9.3.5 The ICT Authority shall collect and analyse statistical data to reaffirm the fairness, validity, reliability, and overall performance of all examinations. Identified deficiencies shall be promptly addressed through documented corrective actions.

9.4 Decision on certification

9.4.1 The ICT Authority shall collect, document, and retain comprehensive information throughout the certification process to:

a) Make informed, evidence-based certification decisions.
b) Maintain traceability for audits, appeals, or complaints.

9.4.2 The ICT Authority shall ensure that all decisions regarding granting, maintaining, recertifying, extending, reducing, suspending, or withdrawing certification are made internally and are not outsourced to any external organization.

9.4.3 The ICT Authority shall limit its certification decisions solely to matters that directly relate to the requirements set forth in the certification scheme.

9.4.4 The ICT Authority shall make all certification decisions solely based on the documented evidence gathered during the certification process. Moreover, those responsible for these decisions shall not have been involved in the candidate's training or examination to ensure complete impartiality.

9.4.5 The ICT Authority shall ensure that individuals responsible for certification decisions possess the necessary expertise and practical experience with the certification process, enabling them to accurately assess whether all certification requirements have been met.

9.4.6 The ICT Authority shall grant certification only after every certification requirement has been fully met.

9.4.7 The ICT Authority shall issue a certificate to every certified individual and maintain exclusive ownership of these certificates. Each certificate, whether in the form of a letter, card, or another approved medium, shall be signed or authorized by a designated responsible member of the Authority's staff.

9.4.8 Each certificate issued by the ICT Authority shall, at a minimum, include the following details:

a) The certified individual's name.
b) A unique identifier.
c) The name of the ICT Authority.
d) A reference to the relevant certification scheme, standard, or other pertinent documents, including the issue date if applicable.
e) A description of the certification scope, including any applicable validity conditions and limitations.
f) The effective date of certification and the expiration date.

9.4.9 The ICT Authority shall design its certificates to minimize the risk of counterfeiting.

9.5 Suspending, withdrawing or reducing the scope of certification

9.5.1 The ICT Authority shall establish a clear policy along with documented procedures for the suspension or withdrawal of certification, or for reducing its scope. These procedures must detail the subsequent actions that will be taken by the Authority.

9.5.2 The ICT Authority shall specify a timeframe within which any issues leading to a suspension shall be resolved. If these issues remain unresolved within that period, the certification shall be withdrawn or the scope of certification shall be reduced.

9.5.3 The ICT Authority shall establish enforceable measures with each certified individual to ensure that, if their certification is suspended, they refrain from promoting or representing themselves as certified during the suspension period.

9.5.4 The ICT Authority shall establish enforceable measures with all certified individuals to ensure that, if their certification is withdrawn, they cease all references to holding a certified status.

9.6 Recertification process

9.6.1 The ICT Authority shall establish documented procedures to implement the recertification process in accordance with the requirements of the certification scheme.

9.6.2 The ICT Authority shall verify during the recertification process that the certified individual continues to demonstrate the required competence and complies with the current scheme requirements.

9.6.3 The recertification period shall be determined according to the requirements of the certification scheme. In establishing this period, the ICT Authority shall consider, the following:

a) Regulatory requirements;
b) Updates to normative documents;
c) Changes in the relevant scheme requirements;
d) The nature and maturity of the industry or field in which the certified individual operates;
e) The risks associated with an incompetent professional;
f) Ongoing technological advancements and evolving requirements for certified professionals;
g) The expectations of interested parties; and
h) The frequency and content of any required surveillance activities.

9.6.4 The ICT Authority shall ensure that the recertification activity or activities selected are sufficient to enable an impartial assessment that confirms the certified individual's ongoing competence.

9.6.5 In accordance with the certification scheme, the ICT Authority shall ensure that the recertification process incorporates, at a minimum, the following elements:

a) On-site assessments.
b) Evaluation of professional development.
c) Structured interviews.
d) Verification of continued satisfactory work and work experience records.
e) Examinations.
f) Assessments of physical capability related to the relevant competence.

9.7 Use of certificates, logos and marks

9.7.1 The ICT Authority shall document clear terms governing the use of its certification mark, including the proper management of rights related to its usage and representation.

9.7.2 The ICT Authority shall require certified individuals to sign an agreement for the following reasons:

a) Adherence to all applicable requirements of the certification scheme;
b) Restriction of certification claims strictly within the scope of certification granted by the ICT Authority;
c) Avoidance of any misuse of certification that damages the ICT Authority's reputation, including refraining from misleading or unauthorized statements about the certification;
d) Immediate cessation of all certification claims referencing the ICT Authority or its certification upon suspension or withdrawal, including the return or destruction of issued certificates;
e) Prohibition use of the certificate in a misleading manner.

9.7.3 The ICT Authority shall address any misuse of its certification mark or logo through corrective actions.

9.8 Appeals against decisions on certification

9.8.1 The ICT Authority has established and maintains a complaints and appeals procedure (ICTA–DPS-CAPA-001) for receiving, evaluating, and resolving appeals. This appeals-handling process includes the following components:

a) Procedures for receiving, validating, and investigating appeals, and for deciding what actions are to be taken in response to it, taking into account the results of previous similar appeals
b) tracking and documentation of all appeals, including actions undertaken to resolve them;
c) ensuring that, where applicable, appropriate corrections and corrective actions are taken.

9.8.2 The implementation of the complaints and appeals procedures (ICTA–DPS-CAPA-001) shall ensure that all appeals are dealt with in a constructive, impartial, and timely manner.

9.8.3 The ICT Authority shall publish without request a description of the appeals-handling process.

9.8.4 The ICT Authority shall be responsible for all decisions at all levels of the appeals-handling process. It shall ensure that personnel responsible for decision-making in the appeals-handling process are independent from those involved in the decision being appealed.

9.8.5 The ICT Authority shall ensure that the submission, investigation, and decision on appeals do not lead to discriminatory actions against the appellant.

9.8.6 The ICT Authority shall acknowledge receipt of the appeal and provide the appellant with progress reports and the outcome

9.8.7 The ICT Authority shall formally notify the appellant of the end of the appeals-handling process.

9.9 Complaints

9.9.1 The ICT Authority has documented complaints and appeals procedures (ICTA–DPS-CAPA-001) for receiving, evaluating, and making decisions on complaints.

9.9.2 The ICT Authority shall ensure that a description of its complaints-handling process is publicly accessible without request. The procedures shall treat all parties fairly and equitably.

9.9.3 The complaints and appeals procedures shall ensure that all complaints are handled and processed in a constructive, impartial, and timely manner. The complaints-handling process shall include the following elements:

a) Defined procedures for receiving, validating, and investigating complaints, and deciding what actions are to be taken in response to it
b) tracking and recording of complaints, including actions undertaken in response to them;
c) ensuring that, where applicable, appropriate corrections and corrective actions are taken.

9.9.4 The ICT Authority shall verify upon receipt of a complaint whether it relates to certification activities for which it is responsible and, if so, shall respond accordingly.

9.9.5 The ICT Authority shall formally acknowledge receipt of the complaint and keep the complainant informed through regular progress updates and timely communication of the final outcome.

9.9.6 The ICT Authority shall assume responsibility for gathering and verifying all necessary information to validate the complaint.

9.9.7 The ICT Authority shall formally notify the complainant of the end of the complaints-handling process.

9.9.8 The ICT Authority shall ensure that any substantiated complaint about a certified person is formally communicated to the person in question at an appropriate time.

9.9.9 The ICT Authority shall ensure that its complaints-handling process is subject to confidentiality requirements, as it relates to both the complainant and the subject of the complaint.

9.9.10 The ICT Authority shall ensure that the decision communicated to the complainant is made or reviewed and approved by personnel who were not previously involved in the subject of the complaint.

10.0 MANAGEMENT SYSTEM REQUIREMENTS

10.1 General

The ICT Authority has established, documented, implemented, and maintained a management system capable of ensuring and evidencing consistent compliance with the requirements of ISO/IEC 17024 Standard. In addition to fulfilling the obligations outlined in Clauses 4 to 9, the ICT Authority has implemented its management system in alignment with the Option specified below:

- A general management system which fulfils the requirements of 10.2

10.2 General management system requirements

10.2.1 General

The ICT Authority shall establish, document, implement, and maintain a management system that effectively supports and demonstrates ongoing compliance with the requirements set forth in ISO/IEC 17024 Standard.

The ICT Authority's top management shall establish and document policies and objectives governing its certification activities.

Top management shall provide evidence of its commitment to developing and implementing a management system that meets ISO/IEC 17024 Standards requirements. Furthermore, the top management shall ensure that the policies are understood, implemented, and maintained across all levels of the organization.

The ICT Authority's top management shall designate a member of management who, irrespective of other responsibilities, shall have the responsibility and authority to:

a) ensure that processes and procedures needed for the management system are established, implemented and maintained;

b) Report to top management on the performance of the management system and any need for improvement.

10.2.2 Management System Documentation

The ICT Authority shall document all applicable requirements of the ISO/IEC 17024 Standard and integrate them into its management system framework. The ICT Authority shall ensure that this documentation is disseminated to all relevant personnel.

10.2.3 Control of documents

The ICT Authority shall establish procedures to govern the control of documents (both internal and external) that relate to meeting the requirements of ISO/IEC 17024 Standard. These procedures shall define controls needed to:

a) approve documents for adequacy prior to issue;
b) review and update as necessary and re-approve documents;
c) ensure that changes and the current revision status of documents are identified;
d) ensure that relevant versions of applicable documents are provided at points of use;
e) ensure that documents remain legible and readily identifiable;
f) ensure that documents of external origin are identified and their distribution controlled;
g) prevent the unintended use of obsolete documents and apply suitable identification if they are retained for any purpose.

10.2.4 Control of records

The ICT Authority has established procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of ISO/IEC 17024 standard.

The ICT Authority has established procedures for retaining records for a period consistent with its contractual and legal obligations. Access to these records shall be consistent with the confidentiality arrangements.

10.2.5 Management review

10.2.5.1 General

The ICT Authority's top management has established procedures to review its management system at planned intervals. These reviews shall ensure the ongoing suitability, adequacy, and effectiveness of the system, including the stated policies and objectives related to the fulfilment of ISO/IEC 17024 Standard. These reviews shall be conducted at least once every 12 months and shall be documented.

10.2.5.2 Review input

The ICT Authority shall ensure that the input to the management review includes the following:

a) results of internal and external audits (e.g., accreditation body assessment)
b) feedback from applicants, candidates, certified persons, and interested parties regarding fulfilment of ISO/IEC 17024 Standard.
c) safeguarding impartiality;
d) the status of preventive and corrective actions;
e) follow-up actions from previous management reviews;
f) the fulfilment of objectives;
g) changes that could affect the management system;
h) appeals and complaints.

10.2.5.3 Review output

The output from the management review shall include as a minimum decisions and actions related to the following:

a) improvement of the effectiveness of the management system and its processes;
b) improvement of the certification services related to the fulfilment of the ISO/IEC 17024 standard;
c) resource needs.

10.2.6 Internal audits

10.2.6.1 The ICT Authority has developed and documented procedures for conducting internal audits to confirm that it meets the requirements of the ISO/IEC 17024 Standard and that its management system is effectively implemented and maintained.

10.2.6.2 The ICT Authority shall design an audit programme that considers the importance of the processes and areas to be audited, as well as the results of previous audits.

10.2.6.3 The ICT Authority shall conduct internal audits at least once every 12 months. However, if it can be demonstrated that its management system is consistently effective and stable in accordance with the ISO/IEC 17024 Standard, the frequency of internal audits may be reduced.

10.2.6.4 The ICT Authority shall ensure that:

a) Internal audits are performed by competent personnel who are knowledgeable in the certification process, auditing and the requirements of the ISO/IEC 17024 Standard;
b) Auditors do not audit their own work;
c) The personnel responsible for the audited areas are informed of the audit outcomes;
d) Any actions resulting from internal audits are implemented promptly and appropriately; and
e) Opportunities for improvement are identified.

10.2.7 Corrective actions

The ICT Authority has developed and documented procedures to identify and manage nonconformities in its operations. Where necessary, it shall take corrective actions to eliminate the causes of these nonconformities to prevent their recurrence, with measures that are appropriate to the impact of the problems encountered. The procedures have defined requirements for the following.

a) identifying nonconformities;
b) determining the causes of nonconformity;
c) correcting nonconformities;
d) evaluating the need for actions to ensure that nonconformities do not recur;
e) determining and implementing the actions needed in a timely manner;
f) recording the results of actions taken;
g) reviewing the effectiveness of corrective actions.

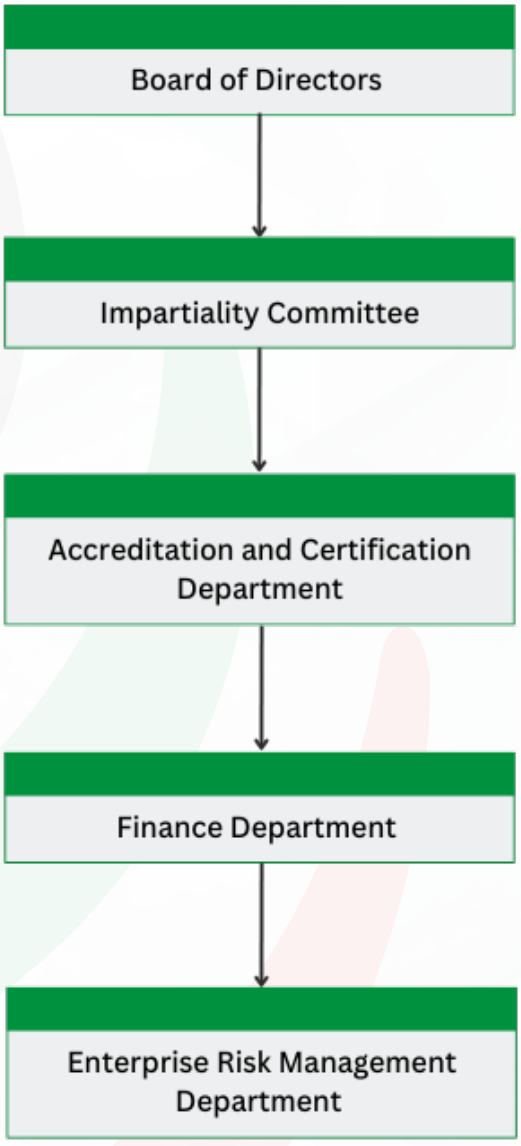
10.2.8 Preventive actions

The ICT Authority has developed and documented procedures for taking preventive actions to eliminate the causes of potential nonconformities. The preventive actions taken shall be appropriate to the probable impact of the potential problems. The procedures for preventive actions have defined requirements for the following:

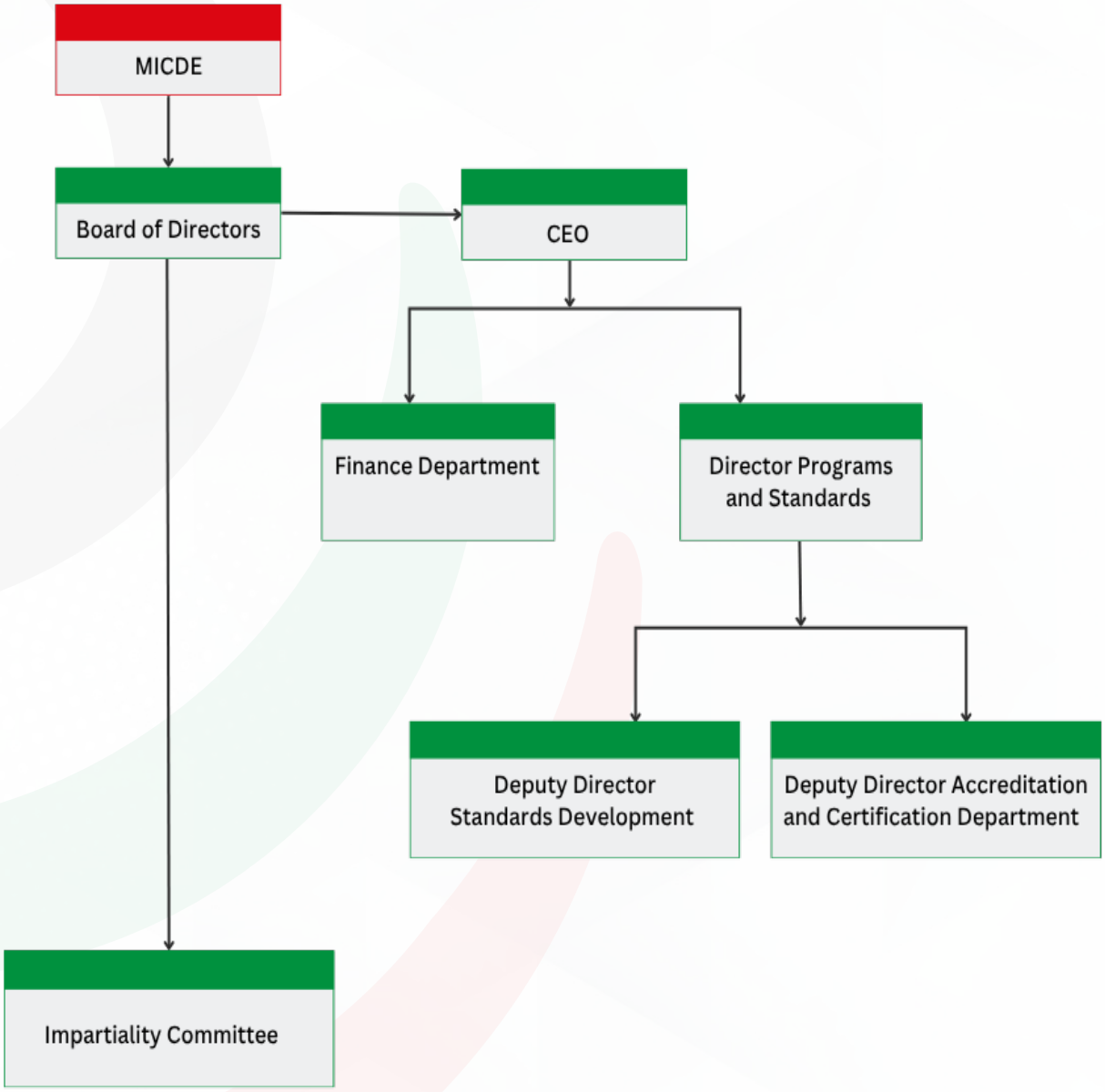
a) identifying potential nonconformities and their causes;
b) evaluating the need for action to prevent the occurrence of nonconformities;
c) determining and implementing the action needed;
d) recording the results of actions taken;
e) reviewing the effectiveness of the preventive actions taken.

11.0 APPENDICES

APPENDIX I: AN ORGANIZATIONAL CHART SHOWING LINES OF AUTHORITY, ROLES



APPENDIX II ORGANIZATIONAL CHART - REPORTING LINES AND INTERACTIONS WITH THE MINISTRY



ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE


ICT
Authority