GOVERNMENT ICT STANDARDS

Systems & Applications Standard

(Enterprise Resource Planning Systems)

ICTA.6.1.001:2026

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

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICT Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

ICT AUTHORITY (ICTA)

Teleposta Towers 12th floor. Kenyatta Avenue
P.O. Box 27150-00200, Nairobi Kenya
Tel.: +254 20 2089061
Web: http://www.icta.go.ke
Email: standards@ict.go.ke

DOCUMENT CONTROL

Document Name:	Enterprise Resource Planning Systems Standard
Prepared by:	Government Enterprise Resource Planning Systems Standard Committee
Edition:	First Edition
Approved by:	Board of Directors
Date Approved:	22nd April 2026
Effective Date:	22nd April 2026
Next Review Date:	After 3 years

CONTENTS

FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology, including systems, infrastructure, processes, human resources, and technology for the public service. The overall purpose of this mandate is to ensure a coherent and unified approach to the acquisition, deployment, management, and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated, and cost-effective deployment and use of ICTs. To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices, as well as relevance to the Kenyan public service. The committee eventually adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In an engagement founded on a memorandum of understanding, KEBS participated in the development of these standards and provided invaluable advice and guidance. For example, the ERP Systems Standard, which falls under the overall Government Enterprise Architecture (GEA), has been prepared in accordance with KEBS standards development guidelines which are, in turn, based on international best practices established by standards development organizations, including ISO. The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for the management, enforcement, and review of this standard. The Directorate shall carry out quarterly audits in all Ministries, Counties, and Agencies (MCA) to determine compliance with this standard. The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services, and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

Jessy Maruti Kiveu
Chief Executive Officer
ICT Authority

1.0 INTRODUCTION

The increasing complexity of ERP systems has created new opportunities while simultaneously introducing significant challenges for organizations that develop, acquire, and use such systems. These challenges occur throughout the entire system life cycle and across all levels of architectural detail. These standards aim to increase the likelihood that acquired ERP systems are fit for purpose, sustainable and secure. The standards also support a clear understanding of, and agreement on, the roles that different Ministries, Counties, Departments, and Agencies (MCDAs) should play in the development or acquisition of ERP systems, and assist MCDAs in understanding and agreeing on appropriate steps within the development process.

This document describes standards for the development (or purchase, configuration, installation, and integration) and the maintenance and management of Enterprise Resource Planning (ERP) systems used for administrative and operational purposes within Government. Responsibility for ERP system development, implementation, and maintenance may be centralized within an ICT department or decentralized across functional departments, depending on the organizational structure. While reference may be made to an "ICT department," these standards apply to any department or any vendor engaged by an MCDA that undertakes the development, configuration, implementation, integration, or maintenance of ERP systems. The applicability of these standards is determined by the nature, scope, and criticality of the ERP system, not by the organizational unit responsible for its implementation.

When determining how these standards apply to ERP systems, the following two characteristics shall be considered:

1. The size and complexity of the ERP system, including the number of modules, integrations, users, and supported business processes.
2. The criticality of the ERP system to the operations of the MCDA or the Government as a whole, and the level of risk associated with unsuccessful implementation or operation.

An ERP system shall be considered high risk if failure to function correctly or to be delivered within the required timeframe could result in a major inability of the MCDA to perform essential functions, a significant financial loss, disruption of core government services, or substantial legal or regulatory exposure.

2.0 SCOPE

The document covers the acquisition, configuration, customization, deployment, operation, integration, maintenance, upgrade, and retirement (whether performed internally or externally to the MCDA) of ERP systems, modules, and related services, including embedded software components and firmware.

Common modules that may be part of an ERP system are described in Annex 1 (Common Modules). This annex provides an overview of typical functionalities for Finance, Human Resources, Procurement, and CRM modules.

Application

This standard applies to:

- Central Government of Kenya
- County Governments
- Constitutional Commissions
- State Corporations

3.0 NORMATIVE REFERENCES

- ISO 9001:2015 – Quality management systems – Requirements
- ISO/IEC 27001 – Information security management
- ISO/IEC 20000-1 – IT service management
- ISO 8000-1 – Data quality
- ICTA Systems & Applications Standard (2023)
- Government Enterprise Architecture (GEA) Framework
- Government ICT Governance Framework

4.0 ABBREVIATIONS AND ACRONYMS

ERP	Enterprise Resource Planning
MCDA	Ministries, Counties, Departments, and Agencies of the Government
SLA	Service Level Agreement
GEA	Government Enterprise Architecture
API	Application Programming Interface
ICT	Information and Communications Technology
MDM	Master Data Management
SSO	Single Sign-On
IDE	Integrated Development Environment
UAT	User Acceptance Test
CMDB	Configuration Management Database
ISO	International Organization for Standardization

5.0 TERMS AND DEFINITIONS

5.1 Enterprise Resource Planning (ERP)

An integrated software system that supports and automates core organizational business processes, including finance, procurement, human resource management, inventory, assets, and reporting, using a shared database and standardized workflows.

5.2 ERP System Governance

The framework of structures, roles, processes, and controls established to direct, manage, and monitor the ERP system throughout its lifecycle to ensure accountability, compliance, and value realization.

5.3 ERP Steering Committee

A senior management committee established to provide strategic oversight, direction, and decision-making authority for the ERP system.

5.4 Business Owner

A senior officer accountable for ensuring that the ERP system delivers the intended business outcomes and supports institutional objectives.

5.5 Business Process Owner

An officer responsible for defining, approving, and maintaining business processes and controls supported by a specific ERP functional area.

5.6 Business Process

A structured set of activities and workflows designed to achieve a specific organizational objective and supported by the ERP system.

5.7 Workflow

A sequence of automated tasks, approvals, and controls configured within the ERP system to execute a business process.

5.8 Segregation of Duties

The division of responsibilities among different users to reduce the risk of error, fraud, or unauthorized actions by ensuring that no single individual controls all critical stages of a transaction.

5.9 Maker-Checker Control

A control mechanism where one user initiates a transaction (maker) and a different authorized user reviews and approves the transaction (checker).

5.10 Third Party
Any external entity, including vendors, system integrators, consultants, or service providers, engaged to supply, implement, support, or maintain the ERP system.

5.11 Third-Party Management
The processes and controls used to govern, monitor, and manage third parties involved in the ERP system to ensure performance, security, and compliance.

5.12 Service Level Agreement (SLA)
A formal agreement defining service performance targets, responsibilities, response times, and penalties applicable to ERP services provided by a third party.

5.13 ERP Configuration
The setup and parameterization of ERP system features and workflows without altering the underlying source code.

5.14 ERP Customization
Modification of ERP source code or core logic to meet specific business requirements beyond standard configuration.

5.15 ERP Support
The set of activities performed to ensure continuous operation of the ERP system, including incident management, problem resolution, maintenance, and user assistance.

5.16 ERP User
Any authorized individual who accesses and performs functions within the ERP system based on assigned roles.

5.17 Super-User
An advanced ERP user with enhanced knowledge and permissions who provides functional support and guidance to other users.

5.18 ERP Administrator
An ICT officer responsible for technical administration, security, access control, and system configuration of the ERP system.

5.19 Training Needs Assessment
A structured evaluation used to identify ERP user roles, required competencies, and training gaps prior to or during ERP implementation.

5.20 Knowledge Transfer

The formal process of transferring skills, system knowledge, and documentation from vendors or consultants to MCDA staff to ensure sustainability and reduce dependency.

5.21 Audit Trail

A secure, chronological record of ERP system activities that enables tracing of transactions, approvals, changes, and user actions.

5.22 Change Management

A controlled process for requesting, reviewing, approving, implementing, and documenting changes to the ERP system.

5.23 Government Enterprise Architecture (GEA)

A standardized framework that guides the design, development, and integration of government information systems to ensure interoperability, consistency, and efficiency.

5.24 GEA

Government Enterprise Architecture

5.25 Clean Data

Data that is accurate, complete, consistent, timely, and valid

5.26 Data Integration

Combining data from different sources into a unified view

5.27 Master Data

Core data entities critical to business operations

5.28 API

Application Programming Interface enabling system communication

5.29 Interoperability

Ability of ICT systems to exchange and use information seamlessly

5.30 Change

Any addition, modification, or removal of an ICT component, process, or service

5.31 Change Request

Formal proposal for a change, documented and submitted for approval

5.32 Change Advisory Board (CAB)

Group responsible for assessing, prioritizing, and approving changes

5.33 User Engagement

Involving end-users in change planning, testing, and implementation

5.34 Adoption Tracking

Monitoring how users accept and use new systems or processes

5.35 Configuration Item (CI)

Component that needs to be managed to deliver an IT service

5.36 Configuration Management Database (CMDB)

Database storing configuration records

5.37 Baseline Configuration

Approved configurations serving as a reference point

5.38 Configuration Control

Process of managing changes to CIs in a controlled manner

5.39 Unauthorized Change

Change made without following approved processes

6.0 REQUIREMENTS

6.1 ERP System Governance

6.1.1 Governance Structure and Roles

i. MCDAs shall establish an ERP Implementation Committee to spearhead implementation of the ERP system.
ii. The ERP Implementation Committee shall report to the ICT steering Committee
iii. Membership of the ERP Implementation Committee shall include Business Process Owners from functions covered by the ERP scope.
iv. The roles and responsibilities of the members of the ERP implementation committee are as provided on Annex 13 (ERP System Governance Roles and Responsibilities).
v. During ERP implementation, the committee shall follow the systems development acceptable procedures as provided on Annex 9 of the Systems and Applications Standard.
vi. The MCDA shall be guided by their approved data management and governance policy, change management policy and configuration management policy to safeguard organizational data, manage changes to ERP and its configurations.

6.1.2 Third-Party Management

6.1.2.1 Acquisition process

i. The acquisition of the ERP system shall shall prioritize configuration/development over customization to reduce long-term vendor dependency.
ii. Any proposed customization shall be presented with a customization impact statement. This document shall include:

a) A business case explaining why configuration or standard functionality cannot meet the requirement.
b) A long-term cost analysis covering increased upgrade complexity, heightened vendor dependency, and ongoing maintenance.
c) A risk assessment on system stability and future upgrade paths.

iii. All Customization Impact Statements shall require written approval from the ICT Steering Committee before development may commence.

6.1.2.2 Contract and SLA Requirements

i. MCDAs shall ensure that all ERP vendors, system integrators, consultants, and service providers are formally engaged through procurement and contracting processes provided for under the relevant procurement law.

ii. Third-party involvement in ERP systems shall be governed by documented contracts and service level agreements.

iii. ERP-related contracts shall include:

i. Scope of services and deliverables;
ii. Roles and responsibilities of each party;
iii. Implementation, methodology, timelines and milestones;
iv. Acceptance and sign-off criteria;
v. Support and maintenance obligations;
vi. Knowledge transfer and training provisions
vii. Security, confidentiality, and data protection requirements;
viii. Exit, transition, and handover arrangements.

iv. MCDAs shall establish Service Level Agreements for ERP third-party services.

v. MCDAs shall ensure that ERP Service Level Agreements are defined and reviewed on an annual basis.

vi. ERP SLAs shall be valid for a period of one (1) year, subject to renewal based on performance evaluation.

vii. Annual SLA reviews shall assess:

a. Compliance with agreed service levels;
b. Incident response and resolution performance;
c. System availability and uptime;
d. User satisfaction;
e. Continued relevance of service levels.

viii. Renewal of ERP SLAs shall be contingent upon satisfactory performance and approval by the ICT Steering Committee.

ix. ERP SLAs shall define:

a. System availability and uptime targets;
b. Incident response and resolution timelines;
c. Escalation procedures;
d. Performance monitoring and reporting requirements;
e. Penalties for non-performance /sustained SLA breaches;
f. Specification of the service/maintenance offered;
g. Change request procedure;

h. Maintenance Schedule and Release Management;
i. Disaster Recovery and Business Continuity plans
j. Sustainability and Handover Plans

6.1.2.3 Local support capacity

a) To ensure timely and effective support, ERP vendors without a primary business presence in Kenya shall demonstrate an established, contractual capacity for local support during procurement and maintain it for the full contract term.

b) Vendors shall fulfill this requirement through a contractual guarantee to deploy certified technical personnel to Kenya within a stringent, guaranteed timeframe for onsite support, with remote support available 24/7. This evidence shall be submitted as part of the technical bid.

6.1.2.4 Source Code, Escrow and Intellectual Property

a) For all custom-developed or significantly customized ERP components, MCDAs shall ensure that ownership of the associated source code and intellectual property is irrevocably and fully assigned to the Government. Contractual clauses shall utilize a present grant of assignment (e.g., "The Vendor hereby assigns…") rather than a mere future promise to assign (e.g., "The Vendor agrees to assign…")

b) Where full ownership is not commercially viable, MCDAs may accept as a minimum the grant of perpetual, irrevocable, royalty-free, and transferable rights to use, modify, maintain, and port the source code for all government purposes. This grant shall survive the termination of the underlying contract.

c) For all mission-critical ERP components (whether custom or core product), MCDAs shall enter into a formal source code escrow agreement with an independent agent. The escrow arrangement shall:

i. Utilize an agent that demonstrates robust security, neutrality, and experience with software assets
ii. Include the complete, buildable source code, all third-party dependencies and licenses, detailed build scripts, deployment instructions, and full technical documentation.
iii. Define unambiguous trigger events, including but not limited to vendor insolvency, material breach of support obligations, failure to correct critical defects, or discontinuation of the product
iv. Require periodic verification by the escrow agent to ensure deposits are complete and functional. The deposit must be updated with every major release and at least biannually.

d) ERP vendors shall not withhold access to source code, technical documentation, or build environments when such access is necessary for the MCDA or its designated agent to:

i. Diagnose and correct critical system defects or security vulnerabilities when the vendor is unable to respond within a contractually mandated critical response period.
ii. Ensure business continuity and facilitate migration following contract expiry, termination, or a validated escrow release event.

e) Where open-source components are used within the ERP system, the vendor shall:

i. Deliver and maintain a comprehensive inventory of all OSS components, including their versions and full license texts.
ii. Warrant that the use and distribution of all OSS components comply with their respective licenses and that the overall license mix does not create conflicts or impose undesirable obligations on the Government.
iii. Indemnify the MCDA against claims arising from OSS license non-compliance.

6.1.2.5 Data Governance and Sovereignty

a) The MCDA is the exclusive controller and steward of all data generated, processed, stored, or transmitted by the ERP system. The MCDA retains all rights, title, and interest in such data as a sovereign asset .

b) ERP vendors and third parties shall act strictly as data processors, handling data solely under the documented instructions of the MCDA and for the explicit purpose of fulfilling the contracted services .

c) ERP vendors and any sub-contractors shall not:

i. Claim any ownership, license, or rights to MCDA data beyond what is strictly necessary for service delivery.
ii. Use, analyze, or process MCDA data for any secondary purpose, including but not limited to training AI/ML models, product improvement, analytics, or commercial exploitation.
iii. Transfer, disclose, or retain MCDA data beyond the authorized service regions or after the service period ends, unless required by law and with immediate notification to the MCDA.

d) ERP contracts shall include explicit, binding provisions for data exit and transition, requiring the vendor to:

i. Upon contract expiry or termination, provide a complete, accurate, and usable copy of all MCDA data. Extracts must be delivered in open, non-proprietary, and machine-readable formats accompanied by a comprehensive data dictionary and schema.
ii. Offer reasonable technical assistance, at a predefined and fair cost, for a period of up to 90 days to support the migration of data to a successor system or service provider.
iii. Upon confirmation of successful data migration by the MCDA, provide a certified statement of the secure and irreversible deletion of all MCDA data from the vendor's production, backup, archival, and disaster recovery systems.

e) Vendor access to MCDA data shall be governed by the principle of least privilege, granted only to identified personnel for defined operational purposes and for a limited duration.

f) All vendor access to data, including administrative, support, and batch processing activities, shall be in line with the information security standards on access management.

Data quality requirements and master data management principles are detailed in Annex 2 (Data Quality Assessment Checklist) and Annex 4 (Master Data Management Framework).

6.1.2.6 Development and Deployment Tools

a) MCDAs shall require that ERP vendors utilize current, vendor-supported, and industry-standard tools, platforms, and frameworks for all development, configuration, customization, and support activities. These technologies must be documented and align with the vendor's own published platform lifecycle.

b) The ERP implementation shall employ a defined set of supporting technologies that ensure project control and security, including:

i. Source & Configuration Control: A version control system for managing all custom code, configuration scripts, and documentation.
ii. Deployment Automation: Tools to automate and standardize deployments across development, testing, and production environments.
iii. Testing Framework: Tools to support automated unit, integration, and performance testing of custom developments.

c) For any custom code or configuration developed, the vendor shall provide the MCDA's ICT staff with:

i. Access to the development and test environments used during the project.
ii. Full technical documentation of the development architecture, coding standards, and build procedures.

d) Knowledge transfer, as mandated in Clause 6.2, shall specifically include comprehensive training for MCDA ICT staff on the development tools, deployment processes, and source code management practices used for the implementation.

e) Vendors shall not implement solutions that create long-term technical lock-in or unsupportable risk. This specifically includes:

i. Unsupported/Obsolete Technologies: Using development tools or frameworks that are outside the vendor's mainstream support lifecycle.
ii. Undocumented "Black Box" Customizations: Deliveries where the internal logic, dependencies, or build process of custom components are not fully documented and transferable to the MCDA.

f) The ERP system interface, configuration, and all associated source code, including but not limited to variable names, function names, comments, documentation strings, database field names, and system messages, shall be written in the English language. This requirement applies to all modules, customizations, integrations, and extensions developed or procured under this standard. Non-English text shall only be permitted where required for localization purposes, such as user-facing translations, and shall not affect the underlying codebase.

6.1.2.7 Implementation Timeline

a. MCDAs shall ensure that ERP implementation contracts define a clear, measurable, and phased implementation timeline, with defined milestones and acceptance criteria for each phase.

b. The total duration for ERP implementation, from contract commencement to final system acceptance, should not to exceed six (6) months. This target is based on the principle of focused delivery to maximize value and minimize business disruption.

c. The ERP implementation timeline shall include, at a minimum, the following phases and activities:

i. Project initiation and planning;
ii. Business process review and system configuration;
iii. System integration, testing, and user acceptance testing (UAT);
iv. Training, knowledge transfer, and business readiness;
v. Go-live and post-implementation stabilization.

d. Any deviation from the contracted timeline, particularly extensions exceeding the recommended six-month target, should trigger a formal review and approval process. This process shall require:

i. A detailed written justification analyzing the root cause of the delay;
ii. A revised project plan with a risk assessment for the new timeline;
iii. Formal review and approval by the ICT Steering Committee;
iv. Contractual variations, if applicable, signed by the Accounting Officer.

6.1.2.8 Licensing and Intellectual Property

a. MCDAs shall maintain an inventory of all ERP licenses and subscriptions.
b. ERP licensing terms shall be transparent, auditable, and compliant with procurement requirements.
c. All data generated, stored, or processed by the ERP system shall remain the property of the MCDA.

6.1.2.9 Access Control for Third Parties

Third-party access to ERP systems shall be in line with clause 11.0 on access control as outlined in the GOK information security standard.

6.1.3 Change and Configuration Management

a. The MCDA shall establish formal change management and configuration management processes.

b. All changes to the ERP system shall follow the approved change management procedures.
Refer to **Annex 5 (Change Request Template)** for the standard change request form.

c. Configuration items (CIs) shall be identified, documented, and maintained in a configuration management database (CMDB). **Refer to Annex 8 (Configuration Item Register Template)** for the CI register template.

d. Configuration changes shall be controlled using a formal request and approval process.
Refer to Annex 9 (Configuration Change Request Form) for the configuration change request form.

e. Regular configuration audits shall be conducted to ensure integrity and compliance.
Refer to Annex 10 (Configuration Audit Checklist) for the audit checklist.

6.1.4 Quality Assurance

MCDAs shall conduct quality assurance activities throughout the ERP lifecycle.
Refer to Annex 11 (ERP Quality Assurance Checklist) for the QA checklist template.

6.2 Training and Support

6.2.1 Knowledge Transfer and Training

a. The MCDA's ICT staff shall work alongside the vendor's implementation team in all key phases, including configuration, integration, data migration, and testing.
b. Vendors shall handover all technical documentation that include, but is not limited to: configuration manuals, integration architecture, and operation manuals.
c. The MCDA shall develop a training and certification plan for its ICT support staff, to be funded as part of the ERP implementation budget.
d. The vendor shall provide or facilitate accredited product certification training for a minimum number of MCDA ICT staff, as agreed in the contract, to achieve recognized competency levels in system administration and development.

6.2.1.1 Training Governance and Principles

a. MCDAs shall establish a structured training program governed by the ICT Steering Committee to ensure user competency and system adoption.
b. ERP system access rights shall only be granted to users who have successfully completed role-specific mandatory training.
c. Training shall be developed and delivered based on a continuous cycle of needs assessment, delivery, validation, and improvement.

6.2.2 Training Needs Analysis

a) A formal Training Needs Analysis (TNA) shall be conducted prior to implementation and repeated following major system upgrades or business process changes.

b) The TNA shall identify and document:

i. All user roles and categories interacting with the system.

ii. The specific competencies, skills, and authorizations required for each role.

iii. Gaps between current and required competency levels.

6.2.3 Tiered Training Curriculum

Based on the TNA, a tiered curriculum shall be developed for the following distinct audiences, with content and depth tailored accordingly:

i. **End-User Training:** Focused on daily transaction processing and task execution within specific modules.

ii. **Super-User Training:** Advanced training for users who will provide first-line support, manage local workflows, and train other end-users.

iii. **Business Process Owner Training:** Training for managers on monitoring performance, running reports, and understanding how the system enforces controls.

iv. **System Administrator & Technical Training:** Advanced technical training for ICT staff on system configuration, security management, backup/restore, and troubleshooting.

6.2.4 Training Delivery and Execution

a. Training delivery shall utilize blended methods appropriate to the audience, such as instructor-led workshops, hands-on practical exercises, e-learning modules, and simulation environments.

b. All training sessions shall be documented, with records maintained of attendance, curriculum, and training materials

6.2.5 Competency Validation and Certification

a. MCDAs shall validate user competency after training completion. Methods may include practical assessments, tests, or supervised task performance.

b. Formal certification or sign-off shall be mandatory for roles with system-wide impact, including:

i. System Administrators

ii. Super-Users

iii. ERP Support Staff

c. Certification records shall be maintained and linked to user access control profiles.

6.2.6 Training Materials and Knowledge Base

a. MCDAs, with vendor support, shall develop and maintain a centralized repository of up-to-date training materials, including:

i. Role-specific user manuals and quick-reference guides.
ii. Standard Operating Procedures (SOPs).
iii. Recorded demonstrations and e-learning content.
iv. Frequently Asked Questions (FAQs).

b. This repository shall be accessible to all relevant users to support continuous learning and just-in-time knowledge retrieval.

6.2.7 Ongoing Awareness and Continuous Training

a. A user awareness program shall communicate the ERP's objectives, benefits, and upcoming changes.

b. A plan for continuous training shall address:

i. Refresher courses for existing users
ii. Training for new staff (onboarding).
iii. Training for new features deployed through upgrades or module additions.

For comprehensive user involvement throughout the training and support lifecycle, refer to Annex 6 (User Engagement Checklist).

6.3 Business Process Alignment

6.3.1 Process Documentation and Review

a. Prior to any system configuration, MCDAs shall conduct a comprehensive review, rationalization, and documentation of all business processes to be supported or automated by the ERP system. Inefficient, redundant, or non-compliant processes shall be redesigned or eliminated.

b. The documented "To-Be" processes shall serve as the blueprint for ERP configuration and shall include:

i. Process objectives
ii. Assigned Process Owner
iii. Inputs/outputs
iv. Roles/responsibilities
v. Key controls, approval points
vi. Alignment with applicable laws, regulations, and government policies.

Refer to Annex 12 (Business Process Documentation and Re engineering Template) for the standard template to document processes.

6.3.2 Process Owner Authority

a. The MCDA shall formally appoint Business Process Owners for each functional area.

b. The Process Owner is the single point of accountability and is responsible for:

i. Defining, reviewing, and approving the business process design for their area.

ii. Ensuring process consistency and standardization across related departments.

iii. Approving all workflow configurations and control mechanisms that affect their process.

iv. Ensuring ongoing compliance with internal controls and audit requirements.

6.3.3 Workflow Configuration and Controls

a. ERP workflows shall be configured to reflect the approved "To-Be" process documentation and the organization's formal delegation of authority framework.

b. The following controls must be configured and enforced within the system:

i. **Segregation of Duties (SoD):** For all critical transactions, no single user shall control all key stages (e.g., initiate, approve, execute, record). SoD conflicts must be identified, documented, and mitigated.

ii. **Maker-Checker:** A dual-authorization control shall be enforced for all high-risk and financially significant transactions.

6.3.4 Process Change Management

a. Any change to a configured ERP workflow, control, or underlying business process shall follow the formal Change Management procedures.

b. All changes require review and approval by the relevant Business Process Owner and, where the change has cross-functional impact, by the ICT Steering Committee.

6.4 ERP Service Operations and Support

6.4.1 Formal Service Management System

a. MCDAs shall establish and maintain a formal Service Management System for the operational ERP, defining policies, processes, and roles for consistent service delivery and support.

b. This system shall integrate with, and not duplicate, the MCDA's existing ICT service management processes.

6.4.2 Multi-Tiered Support Structure

a. A three-tiered support structure shall be established with clear roles and escalation paths:

- **Tier 1 (Help Desk):** Logs all incidents/service requests, provides initial diagnosis, and resolves common user issues.
- **Tier 2 (Functional/Technical):** Provides in-depth support for complex functional errors, configuration issues, and technical troubleshooting. Staffed by MCDA super-users, business analysts, and ICT officers.
- **Tier 3 (Vendor/Expert):** Manages resolution of software defects and complex technical issues requiring vendor intervention, as governed by the Third-Party Support SLA (Clause 6.3.1).

6.4.3 Incident and Service Request Management

a. All user contacts (incidents, service requests) shall be logged in a centralized system with a unique reference number.

b. Incidents shall be classified (e.g., Critical, Major, Minor) and prioritized based on impact and urgency, with defined resolution targets.

c. A formal Problem Management process shall analyze recurring incidents to identify and eliminate root causes.

6.4.4 Support Escalation Procedures

a. Documented escalation procedures shall define time-based triggers (e.g., "escalate to Tier 2 if not resolved within 4 hours") and functional triggers (e.g., "escalate critical financial module incidents directly to the Business Process Owner").

b. These procedures and expected response times shall be communicated to all users.

6.4.5 Performance Monitoring and Reporting

a. Support performance shall be continuously monitored against key metrics, including:

i. First-contact resolution rate.

ii. Mean Time to Acknowledge (MTTA) and Mean Time to Resolve (MTTR) per priority level.

iii. System availability vs. target.

b. Performance reports shall be reviewed quarterly by the ICT Steering Committee and used to drive service improvement initiatives.

6.4.6 Knowledge Management

a. MCDAs shall establish a knowledge base for ERP support and operations.

b. Lessons learned, solutions, and system configurations shall be documented and retained.

c. Knowledge repositories shall be used to reduce reliance on individual staff or vendors.

6.4.7 Post-Implementation Support

a. The ERP vendor shall provide structured post-implementation support, for a minimum period of six (6) months. This period commences only after final system acceptance (as defined in clause c) and is separate from any long-term maintenance agreement.

b. Post-implementation support shall be comprehensive and proactive, encompassing:

i. Resolution of all system bugs, errors, and defects related to the delivered scope at no additional cost. This excludes changes to approved requirements or new feature requests.;

ii. Active monitoring and tuning to ensure the system meets agreed performance, availability, and security baselines.;

iii. Dedicated, rapid-response assistance to end-users, administrators, and business process owners to address operational questions and process issues arising from live use.

c. The post-implementation support period shall be triggered only upon the MCDA's issuance of a Final System Acceptance Certificate. This certificate shall be issued only after verification that:

i. User Acceptance Testing (UAT) has been formally signed off.

ii. All defects classified as Critical or High priority in the UAT phase are resolved and closed.

iii. All core contractual deliverables (system, documentation, initial user training) have been received and accepted.

d. During the post-implementation period, the vendor shall:

i. Provide timely incident resolution in accordance with agreed service levels;

ii. Support configuration adjustments required to stabilize business processes;

iii. Assist in resolving integration, data, and reporting issues arising from live system use.

e. The MCDA shall measure performance via a post implementation Scorecard tracking key metrics like incident resolution time, system availability, and user satisfaction.

f. If the vendor fails to meet the agreed post implementation support obligations, resulting in unresolved defects or system instability, the MCDA shall have the right to:

i. Formally demand a Corrective Action Plan.

ii. Extend the post implementation support period at no additional cost until all performance and stability objectives are consistently met.

iii. Invoke contractual penalties as stipulated in the main agreement.

Refer to Annex 7 (Post-Implementation Review Form) for the structured review template

6.5 Continuous Process Improvement

6.5.1 Performance Monitoring

a. MCDAs shall establish and monitor key performance indicators (KPIs) to assess the efficiency and effectiveness of ERP-enabled business processes.

6.5.2 Review and Optimazation

a. Performance data and user feedback shall be analyzed periodically (e.g., quarterly) by Business Process Owners.

b. Based on this analysis, Process Owners shall initiate improvements through the formal Change Management process to optimize workflows, enhance controls, or better align with evolving policy and regulatory requirements

6.6 Data & Integration

6.6.1 DATA PORTABILITY AND MANAGEMENT

a. Accessibility Principles:

i. MCDAs shall maintain perpetual access to organizational data regardless of contractual status
ii. Data access shall continue uninterrupted during disputes or transition periods
iii. Emergency data extraction capabilities shall be available at all times

b. Portability Requirements:

i. Data shall be stored and exported using open, documented formats
ii. Systems shall support complete and incremental data extraction
iii. Exports shall maintain data integrity and referential consistency
iv. Extraction shall include comprehensive metadata and audit trails

c. Migration Support:

i. Vendors shall provide extraction tools and documentation for data migration
ii. ERP Systems shall support parallel operations during transition periods
iii. Migration strategies shall address data quality and completeness

d. Implementation Verification:

i. Data extraction capabilities shall be demonstrated during procurement
ii. Regular portability testing shall be conducted during operations
iii. Independent verification of data completeness shall be permitted

Data quality must be ensured throughout; refer to Annex 2 (Data Quality Assessment Checklist). Master data management principles are covered in Annex 4 (Master Data Management Framework).

6.6.2 SYSTEM INTEROPERABILITY

a. Interoperability Principles:

i. ERP systems shall be designed for seamless integration with government systems
ii. Systems shall comply with GOK systems and applications interoperability standards
iii. Integration shall support shared service delivery across government

b. Integration Architecture:

i. Systems shall expose documented interfaces for data exchange
ii. Interfaces shall support standard authentication and authorization methods
iii. Systems shall support synchronous and asynchronous interaction patterns

c. Data Exchange Standards:

i. Data exchange shall use structured formats with documented schemas
ii. Secure transmission methods shall be used for all data exchanges
iii. Metadata shall accompany all data exchanges

d. Government Integration:

i. ERP Systems shall integrate with mandated government platforms
ii. Data exchange formats shall align with government data standards
iii. Integration shall be verified through designated certification processes

e. Testing and Monitoring:

i. The ERP Systems shall undergo comprehensive integration testing
ii. Integration health shall be continuously monitored
iii. Performance metrics shall be tracked and reported

For detailed API design and security requirements, refer to Annex 3 (API Design and Security Guidelines).

6.7 ERP Costing And Financial Sustainability

6.7.1 Costing Framework and Governance

a. MCDAs shall establish a comprehensive ERP Costing Framework to ensure financial sustainability throughout the system lifecycle, from acquisition to retirement.

b. Total Cost of Ownership (TCO) shall be the primary basis for all financial planning, encompassing direct and indirect costs across all lifecycle phases.

c. All ERP - related costs shall be documented, approved, and reviewed at least annually by the ICT Steering Committee.

d. Any significant cost variation or escalation shall be documented, justified, and approved prior to implementation, triggering an automatic management review.

6.7.2 Cost Classification Structure

ERP costs shall be categorized and budgeted under the following logical groups:

a. One-Time Implementation Costs:

i. Software Acquisition: ERP application licenses (perpetual or subscription), database licenses, middleware, reporting/analytics tools, and any proprietary software dependencies.

ii. Implementation Services: Project management, business process re-engineering (BPR), system configuration, workflow design, integration development, and data migration (extraction, cleansing, loading, validation).

iii. Infrastructure Setup: Hosting environment (cloud or on-premise), network connectivity upgrades, end-user equipment (workstations, peripherals), and initial security configuration.

iv. Testing and Quality Assurance: System testing, integration testing, User Acceptance Testing (UAT), security testing, and performance testing.

v. Initial Capacity Building: User training, super-user and administrator training, certification programs, and initial knowledge transfer.

b. Recurring Operational Costs (Annual):

i. **Software Maintenance and Support:** Annual maintenance fees, support contracts, and subscription renewals.

ii. **Infrastructure Operations:** Cloud hosting fees, on-premise facility costs, and network bandwidth.

iii. **Licensing Renewals:** Per-user or concurrent user license renewals, database license renewals.

iv. **Business Continuity:** Disaster Recovery infrastructure, backup operations (including offsite/immutable backups), and DR testing.

v. Security Operations: Ongoing cybersecurity monitoring, vulnerability assessments, and compliance audits.

c. Enhancement and Change Costs:

i. **Upgrades and Patches:** Major version upgrades, patch management, and regression testing.

ii. **New Module Implementation:** Costs for adding new functional modules post-go-live.

iii. **Process Improvements:** Change management, workflow optimization, and additional user training for new features.

6.7.3 Cost Estimation and Budgeting

a) During procurement, vendors shall provide a detailed cost breakdown aligned with the classification structure in 6.7.2, covering at minimum the first five years of operation.

b) MCDAs shall prepare a multi-year budget projection based on the vendor's cost breakdown, including realistic escalation factors.

c) The ICT Steering Committee shall approve the budget projection as part of the business case before contract signing.

6.7.4 Financial Sustainability

MCDAs shall ensure long-term financial sustainability by:

i. Securing committed budget for recurrent costs (maintenance, hosting, support) for the system's planned lifecycle.
ii. Establishing a capital replacement for major upgrades or future replacement.
iii. Avoiding unplanned customizations that increase long-term maintenance complexity and cost.
iv. Periodically benchmarking operational costs against industry standards and peer organizations.

ANNEXES

Annex 1: Common Modules

Module	Functionality	Requirement
Finance Module	**General Financial Management**	a) The Finance module shall comply with the National Treasury's accounting standards and regulations. b) All financial transactions shall be captured in real-time with proper audit trails. c) The system shall support both accrual and cash-based accounting as required.
	Budget Management	a) The system shall support budget formulation, approval, execution, and monitoring. b) Budget controls shall be enforced at the commitment, obligation, and payment stages. c) Budget vs. actual reports shall be generated automatically and made available to authorized users.
	Accounts Payable and Receivable	a) All invoices shall be processed electronically with three-way matching (PO, GRN, Invoice). b) Payment runs shall be automated with support for EFT, RTGS, and other payment methods. c) Debtor and creditor aging reports shall be generated regularly.
	Asset Management	a) The system shall maintain a complete fixed asset register with depreciation calculations. b) Asset tracking shall include acquisition, transfer, maintenance, and disposal processes. c) Asset reconciliation shall be performed annually.

Module	Functionality	Requirement
	Financial Reporting	a) The system shall generate standard financial statements (Balance Sheet, Income Statement, Cash Flow). b) Customizable management reports shall be available for decision support. c) All reports shall be exportable in multiple formats (PDF, Excel, CSV).
Human Resources Module	**Employee Management**	a) A centralized employee database shall be maintained with complete employment history. b) The system shall support organizational structures with positions and reporting lines. c) Employee self-service portals shall be provided for personal data updates.
	Recruitment and Onboarding	a) The recruitment process shall be automated from vacancy advertising to appointment. b) Electronic personnel files shall be created during onboarding. c) Background verification processes shall be integrated where applicable.
	Payroll Management	a) The payroll system shall calculate salaries, allowances, deductions, and statutory contributions. b) Integration with bank systems for salary payments shall be secure and automated. c) Payroll reports shall be generated for NSSF, NHIF, KRA, and other statutory bodies.
	Leave Management	a) Electronic leave application and approval workflows shall be implemented. b) Integration with other systems shall be supported. c) Leave balances shall be available in real-time.

Module	Functionality	Requirement
	Staff Performance Management	a) The system shall support performance appraisal cycles with customizable KPIs. b) Performance data shall be linked to training, promotion, and reward systems. c) Confidentiality of performance ratings shall be maintained.
	Training and Development	a) Training needs analysis shall be conducted through the system. b) Training administration, including nominations, approvals, and feedback, shall be automated. c) Training records shall be linked to employee profiles and performance data.
Procurement Module	**Procurement Planning**	a) The system shall support annual procurement planning aligned with budgets. b) Procurement plans shall be published electronically as per the Public Procurement Act. c) Integration between procurement plans and budget systems shall be maintained.
	Sourcing and Tendering	a) The system shall manage the complete tendering process from advertisement to award. b) Electronic bidding shall be supported with secure submission and opening processes. c) Supplier registration and prequalification shall be managed through the system.
	Purchase Order Management	a) Purchase orders shall be electronically generated and approved based on procurement approvals. b) PO tracking shall include delivery, acceptance, and payment status. c) PO amendments shall follow approved change control procedures.

Module	Functionality	Requirement
	Contract Management	a) Purchase orders shall be electronically generated and approved based on procurement approvals. b) PO tracking shall include delivery, acceptance, and payment status. c) PO amendments shall follow approved change control procedures.
	Contract Management	a) The system shall maintain a contract register with key dates, values, and terms. b) Contract performance monitoring shall be conducted through the system. c) Alerts shall be generated for contract renewals, expirations, and compliance requirements.
	Supplier Management	a) A centralized supplier database shall be maintained with performance ratings. b) Blacklisting and debarment processes shall be managed through the system. c) Supplier payments shall be linked to delivery and acceptance documentation.
	Inventory Management	a) The system shall maintain inventory records with real-time stock levels. b) Reorder points and economic order quantities shall be calculated automatically. c) Stocktaking and reconciliation shall be conducted regularly with system support.
CRM Module	**Citizen Engagement Management**	a) The system shall maintain a centralized citizen database with interaction history. b) Multiple channels (web, email, phone, social media, in-person) shall be integrated. c) Citizen segmentation shall be supported for targeted service delivery.

Module	Functionality	Requirement
	Service Request Management	a) Service requests shall be logged, tracked, and resolved through defined workflows. b) Service level agreements (SLAs) shall be monitored and enforced. c) Escalation procedures shall be automated for overdue requests.
	Feedback and Complaints Management	a) Citizens shall be able to submit feedback and complaints through multiple channels. b) Complaints shall be tracked through resolution with response time monitoring. c) Feedback analysis shall inform service improvement initiatives.
	Knowledge Management	a) A knowledge base shall be maintained for common inquiries and resolutions. b) Self-service portals shall be provided for citizen information access. c) Knowledge articles shall be regularly updated based on inquiry patterns.
	Analytics and Reporting	a) The system shall generate reports on service volumes, response times, and satisfaction levels. b) Predictive analytics shall be used for service demand forecasting. c) Dashboards shall be available for real-time performance monitoring.

Annex 2: 2A: Data Quality Assessment Checklist

2A.1 Data Accuracy Assessment

2A.1.1 Source Data Verification

- 2A.1.1.1 Data matches source documents
- 2A.1.1.2 Calculations and derivations correct
- 2A.1.1.3 Historical data consistency maintained
- 2A.1.1.4 Cross-reference validation performed

2A.1.2 Business Rule Compliance

- 2A.1.2.1 Data conforms to business rules
- 2A.1.2.2 Validation rules consistently applied
- 2A.1.2.3 Exception handling documented
- 2A.1.2.4 Rule violations tracked and resolved

2A.2 Data Completeness Assessment

2A.2.1 Mandatory Field Validation

2A.2.1.1 All required fields populated
2A.2.1.2 Null values within acceptable limits
2A.2.1.3 Default values appropriate
2A.2.1.4 Partial data flagged and reviewed

2A.2.2 Record Completeness

- 2A.2.2.1 All expected records present
- 2A.2.2.2 Duplicate records identified
- 2A.2.2.3 Orphan records resolved
- 2A.2.2.4 Data gaps analyzed

2A.3 Data Consistency Assessment

2A.3.1 Cross-System Consistency

- 2A.3.1.1 Data matches across integrated systems
- 2A.3.1.2 Synchronization frequency appropriate
- 2A.3.1.3 Conflict resolution procedures defined
- 2A.3.1.4 Consistency metrics tracked

2A.3.2 Format Consistency

- 2A.3.2.1 Standard formats applied consistently
- 2A.3.2.2 Date/time formats uniform
- 2A.3.2.3 Naming conventions followed
- 2A.3.2.4 Code values standardized

2A.4 Data Timeliness Assessment

2A.4.1 Update Frequency

- 2A.4.1.1 Data updated within agreed SLAs
- 2A.4.1.2 Real-time requirements met
- 2A.4.1.3 Batch processing completed on schedule
- 2A.4.1.4 Stale data identified and addressed

2A.4.1 Update Frequency

- 2A.4.2.1 Data reflects current state
- 2A.4.2.2 Time-sensitive data marked
- 2A.4.2.3 Historical data properly archived
- 2A.4.2.4 Currency metrics monitored

2A.5 Data Validity Assessment

2A.5.1 Business Validity

- 2A.5.1.1 Data within acceptable ranges
- 2A.5.1.2 Business logic validation passed
- 2A.5.1.3 Domain value compliance
- 2A.5.1.4 Contextual validity verified

2A.5.2 Technical Validity

- 2A.5.2.1 Data type compliance
- 2A.5.2.2 Length restrictions enforced
- 2A.5.2.3 Pattern matching successful
- 2A.5.2.4 Referential integrity maintained

2A.6 Data Uniqueness Assessment

2A.6.1 Duplicate Detection

- 2A.6.1.1 Exact duplicates identified
- 2A.6.1.2 Fuzzy matches analyzed
- 2A.6.1.3 Duplicate resolution process followed
- 2A.6.1.4 Prevention mechanisms in place

2A.6.2 Primary Key Integrity

- 2A.6.2.1 Unique identifiers enforced
- 2A.6.2.2 Key assignment controlled
- 2A.6.2.3 Sequence gaps investigated
- 2A.6.2.4 Key management documented

2A.7 Assessment Reporting

2A.7.1 Metrics Calculation

- 2A.7.1.1 Data quality scores calculated
- 2A.7.1.2 Trend analysis performed
- 2A.7.1.3 Benchmark comparisons made
- 2A.7.1.4 Improvement targets set

2A.7.2 Issue Tracking

- 2A.7.2.1 Issues logged and prioritized
- 2A.7.2.2 Root cause analysis completed
- 2A.7.2.3 Corrective actions assigned
- 2A.7.2.4 Resolution verified

2A.8 Continuous Improvement

2A.8.1 Process Review

- 2A.8.1.1 Assessment process evaluated
- 2A.8.1.2 Tool effectiveness reviewed
- 2A.8.1.3 Resource allocation assessed
- 2A.8.1.4 Best practices adopted

2A.8.2 Training and Awareness

- 2A.8.2.1 Staff trained on data quality
- 2A.8.2.2 Data stewards identified
- 2A.8.2.3 Quality culture promoted
- 2A.8.2.4 Success stories shared

Annex 3: API Design and Security Guidelines

3.1 API Design Principles

3.1.1 RESTful API Design

1. Resource Naming:

- Use nouns, not verbs (e.g., /citizens not /getCitizens)
- Plural form for collections (/citizens, /citizens/{id})
- Lowercase with hyphens (/service-requests)

2. HTTP Methods:

- GET: Retrieve resources
- POST: Create new resources
- PUT: Update entire resources
- PATCH: Partial updates
- DELETE: Remove resources

3. Response Codes:

- 200: OK
- 201: Created
- 400: Bad Request
- 401: Unauthorized
- 403: Forbidden
- 404: Not Found
- 429: Too Many Requests
- 500: Internal Server Error

3.1.2 API Versioning

1. Version Strategy:

- URL path versioning: /api/v1/citizens
- Accept header: Accept: application/vnd.govke.v1+json
- No breaking changes in minor versions

2. Deprecation Policy:

- Announce deprecation 6 months in advance
- Support deprecated versions for 12 months
- Provide migration guides

3.1.3 Request/Response Format

1. Request Structure:

```
{
        "metadata": {
        "requestId": "uuid",
        "timestamp": "iso8601",
        "sourceSystem": "system-id"
        },
        "data": { ... }
}
```

2. Response Structure:

```
{
        "metadata": {
        "requestId": "uuid",
        "timestamp": "iso8601",
        "status": "success|error"
        },
        "data": { ... },
        "errors": [ ... ]
}
```

3.2 API Security Guidelines

3.2.1 Authentication

1. OAuth 2.0 Implementation:

- Authorization Code flow for web apps
- Client Credentials for server-to-server
- JWT tokens with 1-hour expiry
- Refresh tokens for session management

2. API Keys:

- Use for server-to-server communication
- Store in secure key management system
- Rotate quarterly or after security incidents

3.2.2 Authorization

1. Role-Based Access Control:

- Define API roles (read, write, admin)
- Scope-based permissions
- Least privilege principle

2. Resource-Level Authorization:

- Validate user access to requested resources
- Implement ownership checks
- Log authorization decisions

3.2.3 Input Validation

1. Schema Validation:

- JSON Schema validation
- Type checking
- Required field validation

2. Content Validation:

- Size limits on requests
- Content-type verification
- Malicious pattern detection

3.2.4 Rate Limiting

1. Limits by Client:

- 1000 requests/minute per API key
- 100 requests/minute per user
- Burst allowance: 20% above limit

2. Response Headers:

X-RateLimit-Limit: 1000
X-RateLimit-Remaining: 950
X-RateLimit-Reset: 1609459200

3.3 API Documentation Standards

4.3.1 OpenAPI Specification

```
# Example OpenAPI 3.0 Structure
openapi: 3.0.3
info:
  title: Government Citizen API
  version: 1.0.0
  description: API for citizen data management
servers:
  - url: https://api.govke.go.ke/v1
paths:
  /citizens:
        get:
        summary: List citizens
        security:
        - bearerAuth: []
        parameters:
        - name: page
        in: query
        schema:
        type: integer
        minimum: 1
        responses:
        '200':
        description: Successful response
```

3.3.2 Documentation Requirements

1. Must Include:

- Authentication methods
- Endpoint descriptions
- Request/response examples
- Error codes and messages
- Rate limiting information

2. Publishing:

- Interactive documentation (Swagger UI)
- PDF reference manual
- Developer portal
- Change logs

3.4 Monitoring and Logging

3.4.1 Logging Requirements

1. Mandatory Log Fields:

- Request ID (correlation ID)
- Timestamp (ISO 8601)
- Client IP/API Key
- User ID (if authenticated)
- Endpoint and method
- Request/response size
- Processing time
- HTTP status code

2. Security Logging:

- Authentication attempts
- Authorization failures
- Input validation failures
- Rate limit violations

3.4.2 Monitoring Metrics

1. Performance Metrics:

- Response time percentiles
- Request rate per endpoint
- Error rate by type
- System resource usage

2. Business Metrics:

- API usage by department
- Most accessed endpoints
- Peak usage patterns
- User satisfaction scores

3.5 Error Handling

3.5.1 Error Response Format


```
{
  "error": {
        "code": "VALIDATION_ERROR",
        "message": "Invalid input parameters",
        "details": [
        {
        "field": "email",
        "issue": "Invalid email format",
        "value": "invalid-email"
        }
        ],
        "requestId": "req_123456",
        "timestamp": "2024-01-15T10:30:00Z"
  }
}
```


3.5.2 Standard Error Codes

VALIDATION_ERROR: Input validation failed
AUTH_REQUIRED: Authentication required
ACCESS_DENIED: Insufficient permissions
RESOURCE_NOT_FOUND: Requested resource not found
RATE_LIMITED: Rate limit exceeded
SERVER_ERROR: Internal server error
MAINTENANCE: System under maintenance

Annex 4: Master Data Management Framework

4.1 Governance Structure

4.1.1 Master Data Domains

1. Citizen Domain:

- National ID number
- Name, date of birth, gender
- Contact information
- Biometric data

2. Organization Domain:

- Organization name and type
- Registration number
- Tax identification number
- Contact persons

3. Location Domain:

- Postal addresses
- Geographic coordinates
- Administrative boundaries
- Property identifiers

4. Product/Services Domain:

- Service codes and descriptions
- Fee structures
- Service levels
- Delivery channels

4.1.2 Data Stewardship Model

Data Owner (Ministry/Department Head):

- Approves data policies
- Allocates resources
- Resolves escalations

Data Steward (Domain Expert):

- Defines data standards
- Monitors data quality
- Approves data changes

Data Custodian (ICT Department):
- Implements technical solutions
- Manages access controls
- Performs backups and recovery

4.2 Master Data Processes

4.2.1 Data Identification and Classification

Step 1: Domain Analysis
- Identify candidate master data entities
- Document business processes
- Map data flows

Step 2: Criticality Assessment
- Business impact assessment
- Regulatory requirements
- Integration dependencies

Step 3: Classification
- Public, Internal, Confidential, Restricted
- Retention periods
- Archive requirements

4.2.2 Data Quality Management

1. Quality Dimensions:
- Accuracy: Match to real-world entities
- Completeness: All required attributes
- Consistency: Uniform across systems
- Timeliness: Up-to-date information

2. Quality Rules:
- Validation rules per domain
- Cross-reference checks
- Periodic audits
- Quality scorecards

4.2.3 Data Lifecycle Management

Phase 1: Creation
- Standardized data capture
- Validation at point of entry
- Audit trail establishment

Phase 2: Maintenance
- Change control procedures
- Version management
- Access logging

Phase 3: Archive/Deletion
- Archive criteria definition
- Secure deletion procedures
- Compliance verification

4.3 Technical Architecture

4.3.1 MDM Hub Architecture

Components:
1. Source Systems: Legacy systems feeding data
2. Integration Layer: ETL/API for data movement
3. MDM Hub: Central repository with golden records
4. Publishing Services: Distribution to consuming systems
5. Data Quality Engine: Validation and cleansing

Deployment Options:
- Registry: Reference only, no storage
- Repository: Central storage with synchronization
- Hybrid: Combination approach

4.3.2 Data Integration Patterns

Pattern 1: Batch Consolidation
- Frequency: Daily/Weekly
- Use: Historical data, reporting
- Tools: ETL, Data Warehouse

Pattern 2: Real-time Synchronization

- Frequency: Event-driven
- Use: Operational systems
- Tools: Messaging, API

Pattern 3: Hybrid Approach

- Real-time for critical data
- Batch for non-critical
- Scheduled reconciliations

4.4 Data Standards

4.4.1 Data Models

Citizen Entity:

```
{
  "citizenId": "string",  // National ID
  "firstName": "string",
  "lastName": "string",
  "dateOfBirth": "date",
  "gender": "enum(M,F)",
  "nationality": "string",  // ISO 3166-1 alpha-3
  "contactPoints": [
            {
            "type": "email|phone|address",
            "value": "string",
            "isPrimary": boolean
            }
  ]
}
```

4.4.2 Code Standards

1. Country Codes: ISO 3166-1 alpha-3
2. Currency Codes: ISO 4217
3. Language Codes: ISO 639-1
4. Date Format: ISO 8601 (YYYY-MM-DD)
5. Time Format: ISO 8601 (HH:MM:SSZ)

Annex 5: Change Request Template

5.1 Change Request Information

Request ID: CR-YYYY-MM-NNNN
Date Submitted: [DD/MM/YYYY]
Submitted By: [Name/Department]
Type: ☐ Emergency ☐ High Priority ☐ Standard ☐ Low Priority

5.2 Change Description

Change Title: [Brief descriptive title]
System/Application: [Name and version]
Module/Component: [Specific area affected]

Detailed Description:
[Provide comprehensive description of the change including what will be different, what problem it solves, and expected outcomes]

Business Justification:
[Explain why this change is necessary, including benefits and alignment with strategic objectives]

5.3 Impact Analysis

5.3.1 Business Impact

- **Affected Business Units:** [List departments/units]
- **User Impact:** [Number of users affected]
- **Process Changes Required:** [Yes/No, details if yes]
- **Training Required:** [Yes/No, details if yes]

5.3.2 Technical Impact

- **Affected Systems:** [List all systems]
- **Integration Points:** [APIs, interfaces, data flows]
- **Infrastructure Requirements:** [Hardware/software needs]
- **Technical Dependencies:** [Prerequisite changes]

5.3.3 Security Impact

- **Security Assessment Required:** ☐ Yes ☐ No
- **Data Classification Affected:** [Public/Internal/Confidential/Restricted]
- **Access Control Changes:** [Yes/No, details]
- **Compliance Implications:** [Legal/regulatory impacts]

5.4 Risk Assessment

Risk Level: ☐ Low ☐ Medium ☐ High ☐ Critical

Risk Category	Description	Probability	Impact	Mitigation Strategy
Technical				
Operational				
Security				
Business				

5.5 Resource Requirements

5.5.1 Personnel

Role	Hours Required	Cost (Ksh)
Project Manager		
Business Analyst		
Developers		
Testers		
Trainers		
Total		

5.5.2 Financial

- **Development Costs:** Ksh [Amount]
- **License Costs:** Ksh [Amount]
- **Infrastructure Costs:** Ksh [Amount]
- **Training Costs:** Ksh [Amount]
- **Total Estimated Cost:** Ksh [Amount]

5.5.3 Timeline

- **Analysis Start:** [Date]
- **Development Start:** [Date]
- **Testing Start:** [Date]
- **Implementation Date:** [Date]
- **Total Duration: [**Number] weeks

5.6 Testing Requirements

Test Environment Required: ☐ Yes ☐ No
User Acceptance Testing Required: ☐ Yes ☐ No

Test Scenarios:

- [Scenario 1]
- [Scenario 2]
- [Scenario 3]

Success Criteria:

- [Criterion 1]
- [Criterion 2]
- [Criterion 3]

5.7 Implementation Plan

5.7.1 Pre-Implementation

- Backup existing system
- Notify all stakeholders
- Prepare rollback plan
- Schedule maintenance window

5.7.2 Implementation Steps

- [Step 1]
- [Step 2]
- [Step 3]

5.7.3 Rollback Plan

Trigger Conditions:

- [Condition 1]
- [Condition 2]

Rollback Steps:

- [Step 1]
- [Step 2]
- [Step 3]

5.9 Approvals

Role	Name	Signature	Date	Comments
Requestor				
Business Owner				
ICT Manager				
Security Officer				
Change Advisory Board				

5.10 Post-Implementation Review

Review Date: [Date]

Review Conducted By: [Name/Committee]

Outcomes:

- Change Successful
- Partially Successful
- Unsuccessful

Lessons Learned:

[Document what worked well and what could be improved]

Follow-up Actions:

[Any additional actions required]

Note: This template must be completed for all changes except minor updates as defined in the Change Management Standard.

Annex 6: User Engagement Checklist

6.1 Pre-Change Engagement

6.1.1 Stakeholder Identification

- 6.1.1.1 Identify all affected user groups
- 6.1.1.2 Document user roles and responsibilities
- 6.1.1.3 Map user workflows and processes
- 6.1.1.4 Identify user representatives for each group
- 6.1.1.5 Document user demographics and characteristics

6.1.2 User Requirements Gathering

- 6.1.2.1 Conduct user interviews/focus groups
- 6.1.2.2 Document current pain points and challenges
- 6.1.2.3 Capture user expectations and success criteria
- 6.1.2.4 Validate requirements with user representatives
- 6.1.2.5 Document user acceptance criteria

6.1.3 Communication Planning

- 6.1.3.1 Develop user communication strategy
- 6.1.3.2 Create communication timeline
- 6.1.3.3 Prepare communication materials
- 6.1.3.4 Identify communication channels
- 6.1.3.5 Assign communication responsibilities

6.2 During Change Development

6.2.1 User Involvement in Design

- 6.2.1.1 Present design concepts to user groups
- 6.2.1.2 Conduct design review sessions
- 6.2.1.3 Collect user feedback on prototypes
- 6.2.1.4 Incorporate user suggestions into design
- 6.2.1.5 Obtain user sign-off on final design

6.2.2 Training Development

- 6.2.2.1 Conduct training needs analysis
- 6.2.2.2 Develop training curriculum with user input
- 6.2.2.3 Create user-friendly training materials
- 6.2.2.4 Develop quick reference guides and job aids
- 6.2.2.5 Identify and train super-users

6.2.3 Progress Communication

- 6.2.3.1 Provide regular progress updates to users
- 6.2.3.2 Share success stories and milestones
- 6.2.3.3 Address user concerns and questions
- 6.2.3.4 Manage user expectations
- 6.2.3.5 Maintain open feedback channels

6.3 Pre-Implementation Engagement

6.3.1 User Acceptance Testing

- 6.3.1.1 Develop UAT test scenarios with users
- 6.3.1.2 Train users on UAT procedures
- 6.3.1.3 Conduct UAT sessions
- 6.3.1.4 Collect and document UAT feedback
- 6.3.1.5 Obtain UAT sign-off from user representatives

6.3.2 Training Delivery

- 6.3.2.1 Schedule training sessions at convenient times
- 6.3.2.2 Deliver role-based training
- 6.3.2.3 Conduct hands-on practice sessions
- 6.3.2.4 Provide multiple training delivery methods
- 6.3.2.5 Assess training effectiveness

6.3.3 Implementation Communication

- 6.3.3.1 Communicate final implementation date
- 6.3.3.2 Provide implementation timeline to users
- 6.3.3.3 Share what to expect during implementation
- 6.3.3.4 Communicate support arrangements
- 6.3.3.5 Address final user concerns

6.4 During Implementation

6.4.1 Go-Live Support

- 6.4.1.1 Provide on-site support during go-live
- 6.4.1.2 Establish help desk for user questions
- 6.4.1.3 Monitor user adoption and issues
- 6.4.1.4 Provide immediate issue resolution
- 6.4.1.5 Collect real-time user feedback

6.4.2 Change Adoption Monitoring

- 6.4.2.1 Track user login and usage patterns
- 6.4.2.2 Monitor completion of key transactions
- 6.4.2.3 Identify users requiring additional support
- 6.4.2.4 Measure against adoption targets
- 6.4.2.5 Document adoption challenges

6.5 Post-Implementation Engagement

6.5.1 User Feedback Collection

- 6.5.1.1 Conduct post-implementation surveys
- 6.5.1.2 Hold feedback sessions with user groups
- 6.5.1.3 Monitor help desk tickets and patterns
- 6.5.1.4 Collect success stories and testimonials
- 6.5.1.5 Document lessons learned

6.5.2 Ongoing Support

6.5.2.1 Provide refresher training as needed
6.5.2.2 Update training materials based on feedback
6.5.2.3 Establish user communities or forums
6.5.2.4 Provide advanced training for power users
6.5.2.5 Maintain user documentation

6.5.3 Continuous Improvement

- 6.5.3.1 Analyze user feedback for improvement areas
- 6.5.3.2 Implement user-suggested enhancements
- 6.5.3.3 Communicate improvements to users
- 6.5.3.4 Measure user satisfaction over time
- 6.5.3.5 Update engagement strategies based on experience

6.6 Engagement Metrics

6.6.1 Participation Metrics

Metric	Target	Actual	Status
User representative participation	100%		
Training attendance	90%		
Feedback response rate	70%		
UAT completion rate	100%		
Super-user identification	5% of users		

6.6.2 Satisfaction Metrics

Metric	Measurement Method	Frequency	Target
User satisfaction	Survey	Post-implementation	80%
Training effectiveness	Assessment	Post-training	85%
System usability	Task completion rate	Monthly	90%
Support satisfaction	Help desk survey	Weekly	85%
Overall engagement	Composite score	Quarterly	75%

6.6.3 Adoption Metrics

Metric	Calculation	Target
Active users	Users logging in weekly	90%
Feature utilization	Key features used regularly	80%
Process compliance	Users following new processes	85%
Self-service usage	Help desk vs. self-resolution	60%
Proficiency level	Advanced feature usage	40%

6.7 Documentation and Reporting

6.7.1 Required Documentation

- 6.7.1.1 User requirements document
- 6.7.1.2 Communication plan
- 6.7.1.3 Training materials and attendance records
- 6.7.1.4 UAT results and sign-off
- 6.7.1.5 Feedback analysis report
- 6.7.1.6 Adoption metrics report
- 6.7.1.7 Lessons learned document

6.7.2 Reporting Schedule

Report	Frequency	Audience	Purpose
Engagement status	Weekly	Project team	Track progress
User feedback sum-mary	Bi-weekly	Steering commit-tee	Identify issues
Adoption metrics	Monthly	Management	Measure success
Satisfaction report	Quarterly	All stakeholders	Overall assess-ment
Lessons learned	Post-implementation	Future projects	Knowledge transfer

Annex 7: Post-Implementation Review Form

7.1 Review Information

Change Request ID: [CR-YYYY-MM-NNNN]
System/Application: [Name]
Change Description: [Brief description]
Implementation Date: [DD/MM/YYYY]
Review Date: [DD/MM/YYYY]
Review Period: [e.g., First 30 days]

Review Team Members:

Name	Role	Department
	Project Manager	
	Business Owner	
	ICT Representative	
	User Representative	
	Security Officer	

7.2 Objectives Achievement Assessment

7.2.1 Original Objectives

[List objectives from Change Request]

7.2.2 Achievement Rating

Objective	Fully Achieved	Partially Achieved	Not Achieved	Comments
Objective 1	☐	☐	☐	
Objective 2	☐	☐	☐	
Objective 3	☐	☐	☐	
Objective 4	☐	☐	☐	

7.2.3 Success Criteria Evaluation

Success Criteria	Met	Partially Met	Not Met	Evidence
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

7.3 Technical Performance Review

7.3.1 System Performance

Metric	Target	Actual	Status
Response time	[Target]	[Actual]	☐ Met ☐ Not Met
Availability	[Target]	[Actual]	☐ Met ☐ Not Met
Error rate	[Target]	[Actual]	☐ Met ☐ Not Met
System stability	[Target]	[Actual]	☐ Met ☐ Not Met

7.3.2 Technical Issues

Issue	Severity	Resolution Status	Root Cause
	High/Med/Low	Resolved/Open	
	High/Med/Low	Resolved/Open	
	High/Med/Low	Resolved/Open	

7.3.3 Integration Performance

Integration Point	Status	Issues	Resolution
	Working/Issues		
	Working/Issues		
	Working/Issues		

7.4 Business Impact Assessment

7.4.1 Process Improvements

Business Process	Before	After Implementation	Improvement

7.4.2 Efficiency Gains

Area	Metric	Before	After	Improvement
Processing time	Hours			
Manual effort	Hours/week			
Error reduction	Error rate			
Throughput	Transactions/day			

7.4.3 Cost-Benefit Analysis

Cost/Benefit	Estimated	Actual	Variance
Development costs	Ksh	Ksh	Ksh
Implementation costs	Ksh	Ksh	Ksh
Operational savings	Ksh	Ksh	Ksh
Efficiency savings	Ksh	Ksh	Ksh
Net Benefit	**Ksh**	**Ksh**	**Ksh**

7.5 User Adoption and Satisfaction

7.5.1 Adoption Metrics

User Group	Total Users	Active Users	Adoption Rate	Target
			%	%
			%	%
			%	%

7.5.2 User Satisfaction

Survey Results: (Attach detailed survey results)
Overall Satisfaction Score: [Score]/100

Key Positive Feedback:

1.
2.
3.

Key Areas for Improvement:

1.
2.
3.

7.5.3 Training Effectiveness

Training Metric	Target	Actual	Status
Users trained	100%	%	☐ Met ☐ Not Met
Training satisfaction	80%	%	☐ Met ☐ Not Met
Post-training competency	85%	%	☐ Met ☐ Not Met

7.6 Risk and Issue Review

7.6.1 Identified Risks

Risk from Change Request	Materialized?	Impact	Mitigation Applied
	Yes/No		
	Yes/No		
	Yes/No		

7.6.2 New Issues Identified

Issue	Category	Severity	Resolution Plan
	Technical/Process/User	High/Med/Low	
	Technical/Process/User	High/Med/Low	
	Technical/Process/User	High/Med/Low	

7.7 Support and Operations

7.7.1 Support Requirements

Support Area	Pre-Implementation Estimate	Actual Requirement	Gap
Help desk calls	[Number]	[Number]	[Number]
On-site support	[Hours]	[Hours]	[Hours]
Training requests	[Number]	[Number]	[Number]

7.7.2 Documentation Status

Document	Required	Completed	Quality Rating
User manual	Yes/No	Yes/No	Good/Fair/Poor
Technical guide	Yes/No	Yes/No	Good/Fair/Poor
Process flows	Yes/No	Yes/No	Good/Fair/Poor
Trouble-shooting guide	Yes/No	Yes/No	Good/Fair/Poor

7.8 Compliance and Security

7.8.1 Security Assessment

Security Control	Implemented?	Tested?	Issues
Access controls	Yes/No	Yes/No	
Audit logging	Yes/No	Yes/No	
Data protection	Yes/No	Yes/No	
Compliance checks	Yes/No	Yes/No	

7.8.2 Compliance Status

Regulation/Standard	Compliance Status	Issues	Actions Required
Data Protection Act	Compliant/Partial/Non-compliant		
ICT Standards	Compliant/Partial/Non-compliant		
Sector regulations	Compliant/Partial/Non-compliant		

7.9 Overall Assessment

7.9.1 Success Rating

Overall Success: ☐ Highly Successful ☐ Successful ☐ Partially Successful ☐ Unsuccessful

Key Success Factors:

1.
2.
3.

Main Challenges:

1.
2.
3.

7.9.2 Return on Investment

ROI Calculation:

- Total Benefits: Ksh [Amount]
- Total Costs: Ksh [Amount]
- Net Benefit: Ksh [Amount]
- ROI: [Percentage]%

Payback Period: [Number] months

7.10 Recommendations and Actions

7.10.1 Immediate Actions

Action	Owner	Due Date	Priority
			High/Med/Low
			High/Med/Low
			High/Med/Low

7.10.2 Long-term Recommendations

Recommendation	Benefit	Effort	Priority
		High/Med/Low	High/Med/Low
		High/Med/Low	High/Med/Low
		High/Med/Low	High/Med/Low

7.10.3 Process Improvements

Process Area	Improvement Suggested	Expected Benefit
Change management		
User engagement		
Testing approach		
Implementation planning		

7.11 Sign-off

Review Completed By:

Name	Role	Signature	Date
	Project Manager		
	Business Owner		
	ICT Representative		

Approved By:

Name	Role	Signature	Date
	Department Head		

Next Review Date: [DD/MM/YYYY]

Distribution List:

- Change Advisory Board
- Project Steering Committee
- Department Heads
- ICT Authority

Note: This review must be completed within 30 days of implementation for all high-priority changes and within 60 days for standard changes.

Annex 8: Configuration Item (CI) Register Template

8.1 CI Identification

Configuration Item ID: [CI-YYYY-DEPT-TYPE-NNNN]
System/Application: [System Name]
CI Category: ☐ Hardware ☐ Software ☐ Documentation ☐ Service
Criticality Level: ☐ Critical ☐ High ☐ Medium ☐ Low
Owner: [Name/Department]
Date Registered: [DD/MM/YYYY]

8.2 Basic CI Information

Field	Value
CI Name	[Descriptive Name]
Version/Model	[Version Number/Model]
Serial Number	[Manufacturer Serial]
Asset Tag	[Organization Asset Tag]
Manufacturer	[Company Name]
Vendor/Supplier	[Supplier Name]
Purchase Date	[DD/MM/YYYY]
Warranty Expiry	[DD/MM/YYYY]
Location	[Physical Location]
Department	[Owning Department]

8.3 Technical Specifications

8.3.1 Hardware Specifications (if applicable)

Processor: [Type and Speed]
Memory: [Size and Type]
Storage: [Capacity and Type]

Network: [Interface Types and Speeds]
Operating System: [OS Name and Version]
Power Requirements: [Voltage/Amperage]
Physical Dimensions: [Height/Width/Depth]
Weight: [kg]

8.3.2 Software Specifications (if applicable)

Software Type: ☐ Operating System ☐ Application ☐ Database ☐ Middleware
Version: [Major.Minor.Patch]
License Type: ☐ Commercial ☐ Open Source ☐ Freeware
License Key: [Key/Serial Number]
Installation Date: [DD/MM/YYYY]
Supported Until: [DD/MM/YYYY]
Vendor Support Contact: [Details]

8.3.3 Documentation Specifications (if applicable)

Document Type: ☐ User Manual ☐ Technical Guide ☐ Policy ☐ Procedure
Format: ☐ PDF ☐ Word ☐ HTML ☐ Hardcopy
Version: [Document Version]
Author: [Name/Department]
Approval Date: [DD/MM/YYYY]
Review Date: [DD/MM/YYYY]

8.4 Relationships and Dependencies

Parent CI ID	Relationship Type	Description
	Part of/Connected to/Depends on	
	Part of/Connected to/Depends on	

8.4.2 Child CIs

Child CI ID	Relationship Type	Description
	Contains/Connects to/Supports	
	Contains/Connects to/Supports	

8.4.3 Dependencies

Dependent CI	Dependency Type	Criticality
	Required for operation	High/Med/Low
	Required for maintenance	High/Med/Low
	Required for security	High/Med/Low

8.5 Configuration Details

8.5.1 Current Configuration

Configuration Baseline: [Baseline ID]
Configuration Version: [Version]
Last Configured: [DD/MM/YYYY]
Configured By: [Name]
Configuration File Location: [Path/URL]
Hash/Checksum: [Value]

8.5.2 Configuration Parameters

Parameter	Value	Default	Modified
			Yes/No
			Yes/No
			Yes/No

8.5.3 Installed Components

Component	Version	Install Date	Status
			Active/Inactive
			Active/Inactive
			Active/Inactive

8.6 Operational Information

8.6.1 Service Level Agreement

Availability Requirement: [% uptime]
Response Time: [Maximum acceptable]
Support Hours: [e.g., 24/7, Business Hours]
Maintenance Window: [Day/Time]
Backup Schedule: [Frequency and Type]
Recovery Time Objective: [Maximum time]
Recovery Point Objective: [Maximum data loss]

8.6.2 Maintenance Information

Maintenance Type	Schedule	Last Performed	Next Due
Preventive			
Corrective			
Updates			
Backups			

8.7 Security Information

8.7.1 Access Controls

Administrative Access: [Users/Roles]
User Access: [Users/Roles]
Authentication Method: [e.g., Password, Certificate]
Authorization Levels: [Read/Write/Admin]
Access Logging: Enabled/Disabled

8.7.2 Security Configuration

Security Setting	Value	Compliance
Encryption	Enabled/Disabled	Compliant/Non-compliant
Firewall Rules	[Details]	Compliant/Non-compliant
Antivirus	[Details]	Compliant/Non-compliant
Audit Logging	Enabled/Disabled	Compliant/Non-compliant

8.8 Lifecycle Information

8.8.1 Current Status

Status: ☐ Operational ☐ Under Maintenance ☐ Retired ☐ Disposed
Status Date: [DD/MM/YYYY]
Status Changed By: [Name]

8.8.2 Lifecycle Dates

Lifecycle Stage	Planned Date	Actual Date
Procurement		
Installation		
Commissioning		
Operational		
End of Support		
Retirement		
Disposal		

8.8.3 Financial Information

Cost Type	Amount (Ksh)	Date
Purchase Price		
Installation Cost		
Maintenance Cost (Annual)		
Upgrade Cost		
Total Cost of Ownership		

8.9 Change History

8.9.1 Recent Changes

Date	Change Type	Description	Changed By	Approval
	Configuration/Upgrade/ Repair			CR-XXXX
	Configuration/Upgrade/ Repair			CR-XXXX

8.9.2 Audit Trail

Audit Date	Auditor	Findings	Actions Required

8.10 Supporting Documentation

Attached Documents:

- Installation Guide
- Configuration Manual
- Technical Specifications
- License Agreement
- Support Contract
- Maintenance Records
- Security Assessment

Document Locations:

- **Physical Location:** [File Path/Cabinet]
- **Electronic Location:** [URL/Network Path]
- **Backup Location:** [Secondary Storage]

8.11 Verification and Approval

8.11.1 Data Verification

Verified By: [Name]
Verification Date: [DD/MM/YYYY]
Verification Method: ☐ Physical Inspection ☐ System Check ☐ Documentation Review
Accuracy Rating: ☐ 100% ☐ >90% ☐ <90%

8.11.2 Approvals

Role	Name	Signature	Date
CI Owner			
ICT Manager			
Configuration Manager			

8.12 Review Schedule

Next Review Date: [DD/MM/YYYY]
Review Frequency: ☐ Monthly ☐ Quarterly ☐ Bi-annually ☐ Annually
Review Responsibility: [Role/Department]

Review Checklist:

- CI information current and accurate
- Relationships and dependencies updated
- Configuration matches baseline
- Security settings compliant
- Lifecycle status correct
- Documentation complete

Annex 9: Configuration Change Request Form

9.1 Request Information

Request ID: CCR-YYYY-MM-NNNN
Date: [DD/MM/YYYY]
Request Type: ☐ New Configuration ☐ Modification ☐ Correction ☐ Emergency
Priority: ☐ Emergency ☐ High ☐ Medium ☐ Low
CI ID: [CI-XXXX]
CI Name: [Configuration Item Name]

9.2 Requester Information

Requested By: [Name]
Department: [Department Name]
Contact: [Phone/Email]
Role: [Job Title/Role]

9.3 Change Details

9.3.1 Current Configuration

Description: [Describe current configuration state]

Current Settings/Parameters:
[Detailed current configuration]

Documentation Reference: [Document/Version]

9.3.2 Proposed Change

Change Description: [Detailed description of proposed change]

Reason for Change:
☐ Bug Fix ☐ Performance Improvement ☐ Security Update
☐ New Requirement ☐ Compliance Requirement ☐ Other: _____
Business Justification: [Explain why change is necessary]
Expected Benefits:

- [Benefit 1]
- [Benefit 2]
- [Benefit 3]

9.3.3 Proposed Configuration

New Settings/Parameters:
[Detailed new configuration]

Configuration Files Affected:
- [File 1] - [Path/Location]
- [File 2] - [Path/Location]
- [File 3] - [Path/Location]

9.4 Impact Analysis

9.4.1 Technical Impact

Affected Systems/Components:
- [System/Component 1]
- [System/Component 2]
- [System/Component 3]

Integration Points Affected:
- [Integration 1]
- [Integration 2]

Performance Impact: ☐ None ☐ Minimal ☐ Moderate ☐ Significant
Estimated Downtime: [Hours/Minutes]

9.4.2 Business Impact

Affected Business Processes:
- [Process 1]
- [Process 2]

User Impact: [Number of users affected]
Timing Considerations: [Optimal timing for change]

9.4.3 Risk Assessment

Risk Level: ☐ Low ☐ Medium ☐ High ☐ Critical

Potential Risk	Probability	Impact	Mitigation Strategy
	Low/Med/High	Low/Med/High	
	Low/Med/High	Low/Med/High	
	Low/Med/High	Low/Med/High	

9.5 Implementation Plan

9.5.1 Proposed Schedule

Planning Start: [Date]
Implementation Date: [Date]
Implementation Time: [Start Time] to [End Time]
Duration: [Hours]
Maintenance Window Required: ☐ Yes ☐ No
If Yes: [Date and Time]

9.5.2 Implementation Steps

- 1[Step 1 - Pre-implementation checks]
- [Step 2 - Backup current configuration]
- [Step 3 - Apply changes]
- [Step 4 - Verification]
- [Step 5 - Post-implementation testing]

9.5.3 Rollback Plan

Trigger Conditions for Rollback:

- [Condition 1]
- [Condition 2]
- [Condition 3]

Rollback Steps:

- [Step 1]
- [Step 2]
- [Step 3]

Estimated Rollback Time: [Hours/Minutes]

9.6 Testing Requirements

9.6.1 Test Environment

Test Environment Required: ☐ Yes ☐ No
If Yes: [Environment Details]

9.6.2 Test Cases

Test Case	Description	Success Criteria
TC-1	[Test description]	[Criteria]
TC-2	[Test description]	[Criteria]
TC-3	[Test description]	[Criteria]

9.6.3 Acceptance Criteria

Technical Acceptance:

- Configuration applied successfully
- System functions as expected
- No adverse performance impact
- Integration points working

Business Acceptance:

- Business processes unaffected
- Users can perform required tasks
- Expected benefits realized

9.7 Resource Requirements

9.7.1 Personnel

Role	Hours Required	Responsible Person
Configuration Manager		
System Administrator		
Tester		
Business Representative		

9.7.2 Tools and Software

Required Tools:

- [Tool 1]
- [Tool 2]

Software Requirements:

- [Software 1] - [Version]
- [Software 2] - [Version]

9.8 Communication Plan

9.8.1 Stakeholders to Notify

Stakeholder	Notification Method	Timing
	Email/Meeting/Portal	Before/During/After
	Email/Meeting/Portal	Before/During/After

9.8.2 Communication Schedule

Pre-implementation: [Date/Time]
During implementation: [Date/Time]
Post-implementation: [Date/Time]

9.8 Approval Section

9.8.1 Technical Review

Reviewed By (Technical Lead): [Name]
Date: [Date]
Recommendation: ☐ Approve ☐ Approve with Conditions ☐ Reject
Comments: [Technical feedback]

9.8.2 Security Review

Reviewed By (Security Officer): [Name]
Date: [Date]
Security Assessment: ☐ Compliant ☐ Non-compliant
Security Conditions: [Any security requirements]

9.8.3 Business Approval

Approved By (Business Owner): [Name]
Date: [Date]
Business Priority: ☐ High ☐ Medium ☐ Low
Comments: [Business considerations]

9.8.4 Configuration Control Board Approval

CCB Decision: ☐ Approved ☐ Approved with Conditions ☐ Rejected ☐ Deferred
CCB Meeting Date: [Date]
CCB Reference: [Meeting Minutes Reference]

Special Conditions/Instructions:

[Any special instructions from CCB]

9.10 Implementation Record

9.10.1 Implementation Details

Implemented By: [Name]
Implementation Date: [Date]
Actual Start Time: [Time]
Actual End Time: [Time]
Actual Duration: [Duration]

9.10.2 Implementation Results

Status: ☐ Successful ☐ Partially Successful ☐ Failed
Issues Encountered: [Details]
Deviations from Plan: [Any deviations]

9.10.3 Verification Results

Verified By: [Name]
Verification Date: [Date]
All Tests Passed: ☐ Yes ☐ No
If No: [Failed tests and reasons]

9.11 Post-Implementation Review

9.11.1 Business Verification

Verified By (Business): [Name]
Date: [Date]
Business Acceptance: ☐ Accepted ☐ Not Accepted
Comments: [Business feedback]

9.11.2 Lessons Learned

What Went Well:
- [Point 1]
- [Point 2]

Areas for Improvement:
- [Point 1]
- [Point 2]

9.11.3 Final Sign-off

Configuration Manager: [Name/Signature/Date]
Change Requestor: [Name/Signature/Date]
Business Owner: [Name/Signature/Date]

Annex 10: Configuration Audit Checklist

10.1 Audit Information

Audit ID: CA-YYYY-MM-NNNN
Audit Date: [DD/MM/YYYY]
Audit Type: ☐ Regular ☐ Ad-hoc ☐ Post-change ☐ Compliance
Audit Scope: [Systems/Applications covered]
Auditor(s): [Names]
Auditee: [Department/Team]

10.2 Preparation Phase

10.2.1 Pre-Audit Documentation

- 6C.2.1.1 Audit notice issued to auditee
- 6C.2.1.2 Audit scope and objectives defined
- 6C.2.1.3 Audit plan developed and approved
- 6C.2.1.4 Audit team briefed on objectives
- 6C.2.1.5 Previous audit findings reviewed

10.2.2 Data Collection

- 6C.2.2.1 Configuration baseline documents obtained
- 6C.2.2.2 Change request records collected
- 6C.2.2.3 Configuration item register accessed
- 6C.2.2.4 System inventory lists verified
- 6C.2.2.5 Access to live systems arranged

10.3 Configuration Documentation Audit

10.3.1 Configuration Item Register

- 6C.3.1.1 All CIs documented in register
- 6C.3.1.2 CI details complete and accurate
- 6C.3.1.3 Relationships and dependencies documented
- 6C.3.1.4 Lifecycle status current
- 6C.3.1.5 Ownership clearly assigned

10.3.2 Configuration Baselines

- 6C.3.2.1 Baselines established for all critical CIs
- 6C.3.2.2 Baselines version controlled
- 6C.3.2.3 Baseline documentation complete
- 6C.3.2.4 Baseline approval records maintained
- 6C.3.2.5 Baseline storage secure and accessible

10.3.3 Change Documentation

- 6C.3.3.1 All changes documented with CCR forms
- 6C.3.3.2 Change approvals properly recorded
- 6C.3.3.3 Implementation records complete
- 6C.3.3.4 Post-implementation reviews conducted
- 6C.3.3.5 Emergency change procedures followed

10.4 Configuration Compliance Audit

10.4.1 Configuration vs Baseline

- 6C.4.1.1 Compare live configuration with baseline
- 6C.4.1.2 Document all variances
- 6C.4.1.3 Verify approved changes match CCRs
- 6C.4.1.4 Check for unauthorized changes
- 6C.4.1.5 Validate configuration backups

10.4.2 Policy Compliance

- 6C.4.2.1 Configurations comply with security policies
- 6C.4.2.2 Configuration standards followed
- 6C.4.2.3 Naming conventions adhered to
- 6C.4.2.4 Documentation standards met
- 6C.4.2.5 Regulatory requirements satisfied

10.4.3 Access Control Verification

- 6C.4.3.1 Configuration access restricted appropriately
- 6C.4.3.2 Segregation of duties maintained
- 6C.4.3.3 Access logs reviewed for anomalies
- 6C.4.3.4 Privileged account usage monitored
- 6C.4.3.5 Access reviews conducted regularly

10.5 Technical Configuration Audit

10.5.1 Server Configuration

- 6C.5.1.1 Operating system patches current
- 6C.5.1.2 Security settings configured properly
- 6C.5.1.3 Unnecessary services disabled
- 6C.5.1.4 User accounts properly managed
- 6C.5.1.5 Audit logging enabled and configured

10.5.2 Network Configuration

- 6C.5.2.1 Firewall rules appropriate and documented
- 6C.5.2.2 Network device configurations secure
- 6C.5.2.3 VLAN configurations proper
- 6C.5.2.4 Routing tables correct
- 6C.5.2.5 Network services properly configured

10.5.3 Application Configuration

- 6C.5.3.1 Application settings match requirements
- 6C.5.3.2 Database configurations optimal
- 6C.5.3.3 Middleware properly configured
- 6C.5.3.4 Integration points working correctly
- 6C.5.3.5 Performance settings appropriate

10.6 Process Compliance Audit

10.6.1 Change Management Process

- 6C.6.1.1 All changes follow approved process
- 6C.6.1.2 Emergency changes properly documented
- 6C.6.1.3 Change windows respected
- 6C.6.1.4 Testing performed before implementation
- 6C.6.1.5 Rollback plans developed and tested

10.6.2 Release Management

- 6C.6.2.1 Configuration changes bundled into releases
- 6C.6.2.2 Release documentation complete
- 6C.6.2.3 Release testing comprehensive
- 6C.6.2.4 Release deployment controlled
- 6C.6.2.5 Release verification performed

10.6.3 Configuration Management Process

- 6C.6.3.1 CI identification process followed
- 6C.6.3.2 Configuration control procedures effective
- 6C.6.3.3 Status accounting accurate
- 6C.6.3.4 Verification and audit conducted regularly
- 6C.6.3.5 Process improvements implemented

10.7 Security Configuration Audit

10.7.1 Security Settings

- 6C.7.1.1 Password policies enforced
- 6C.7.1.2 Encryption properly configured
- 6C.7.1.3 Security patches applied
- 6C.7.1.4 Antivirus/malware protection current
- 6C.7.1.5 Intrusion detection configured

10.7.2 Vulnerability Management

- 6C.7.2.1 Regular vulnerability scans conducted
- 6C.7.2.2 Vulnerabilities tracked and remediated
- 6C.7.2.3 Configuration hardening applied
- 6C.7.2.4 Security baselines maintained
- 6C.7.2.5 Compliance with security standards

10.8 Findings and Observations

10.8.1 Compliance Findings

Finding	CI Affected	Severity	Evidence	Requirement
		High/Med/Low		
		High/Med/Low		
		High/Med/Low		

10.8.2 Non-compliance Issues

Finding	CI Affected	Severity	Evidence

10.8.3 Best Practices Observed

Practice	Example	Benefit

10.9 Recommendations

10.9.1 Immediate Actions Required

Action	Responsible	Due Date	Priority
			High
			High
			High

10.9.2 Medium-term Improvements

Improvement	Benefit	Effort	Timeline
		High/Med/Low	[Months]
		High/Med/Low	[Months]
		High/Med/Low	[Months]

10.9.3 Long-term Recommendations

Recommendation	Strategic Impact	Implementation Timeline
		[Quarters]
		[Quarters]
		[Quarters]

10.10 Audit Reporting

10.10.1 Summary Statistics

Total CIs Audited: [Number]
Compliance Rate: [Percentage]
Critical Findings: [Number]
High Priority Findings: [Number]
Medium Priority Findings: [Number]
Low Priority Findings: [Number]

10.10.2 Overall Assessment

Configuration Management Maturity: ☐ Initial ☐ Repeatable ☐ Defined ☐ Managed ☐ Optimized
Compliance Status: ☐ Fully Compliant ☐ Mostly Compliant ☐ Partially Compliant ☐ Non-compliant
Risk Level: ☐ Low ☐ Medium ☐ High ☐ Critical

10.10.3 Audit Conclusion

Strengths Identified:

1.
2.
3.

Major Concerns:

1.
2.
3.

Overall Opinion: [Summary statement]

10.11 Follow-up Actions

10.11.1 Corrective Action Plan

Finding	Corrective Action	Owner	Due Date	Status
				Open/Closed
				Open/Closed
				Open/Closed

10.11.2 Management Response

Response By: [Name/Title]
Response Date: [Date]
Agreement with Findings: ☐ Fully ☐ Partially ☐ Not Agree
Action Plan Approval: ☐ Approved ☐ Rejected ☐ Modified

10.11.3 Verification Schedule

Next Audit Date: [Date]
Progress Review Date: [Date]
Verification of Actions: [Date]

10.12 Sign-off

10.12.1 Auditor Sign-off

Lead Auditor: [Name/Signature/Date]
Audit Team Members: [Names/Signatures]

10.12.2 Auditee Acknowledgement

Department Head: [Name/Signature/Date]
Configuration Manager: [Name/Signature/Date]

10.12.3 Management Approval

ICT Manager: [Name/Signature/Date]

10.13 Distribution List

Report Distributed To:

- Configuration Control Board
- ICT Management
- Department Heads
- Security Officer
- Quality Assurance Department
- Internal Audit Department

Storage Location: [Document Management System Path]
Retention Period: [Number] years

Note: This audit checklist must be completed for all configuration audits. Findings must be addressed within agreed timelines, and corrective actions verified.

Annex 11: ERP quality assurance (QA) checklist-template

Organization: _____
ERP System: _____
Version: _____ **Date:** _____

This section summarizes overall ERP Quality Assurance compliance based on completed QA checklists.

QA Area	Total Checks	Compliant	Non-Compliant	Compliance %
Governance				
Requirements & Design				
Configuration & Build				
Data Migration				
Testing & Validation				
Security Controls				
Training & Readiness				
Go-Live Readiness				
Post-Implementation Review				

ERP Quality Assurance (QA) checklist

1. General Information

QA Area	Total Checks
MCDA Name	
ERP System Name	
ERP Modules	
Implementation Phase	
QA Review Period	
QA Lead	
Vendor / Integrator	
Date	

2. Governance QA

No	Requirement	Compliant (Yes/No)	Evidence	Remarks
1				
2				
3				
4				
5				
6				
7				

3. Requirements & Design QA

No	Checkpoint	Compliant (Yes/No)	Evidence	Comments
1				
2				
3				
4				
5				
6				

4. Configuration & Build QA

No	Checkpoint	Compliant (Yes/No)	Evidence	Comments
1				
2				
3				
4				
5				
6				

5. Data Migration & Quality QA

No	Checkpoint	Compliant (Yes/No)	Evidence	Comments
1				
2				
3				
4				
5				
6				

6. Testing & Validation QA

No	Test Type	Completed (Yes/No)	Evidence / Report Ref	Comments
1				
2				
3				
4				
5				
6				

7. Security & Control QA

No	Control	Compliant (Yes/No)	Evidence	Comments
1				
2				
3				
4				
5				
6				

8. Training & User Readiness QA

No	Checkpoint	Compliant (Yes/No)	Evidence	Comments
1				
2				
3				
4				
5				
6				

9. Go-Live Readiness Assessment

No	Criterion	Ready (Yes/No)	Remarks
1			
2			
3			
4			
5			
6			

10. Post-Implementation Review

No	Area	Satisfactory (Yes/No)	Findings / Actions
1			
2			
3			
4			
5			
6			

11. Non-Compliance & Corrective Actions

No	Description	Risk Level	Corrective Action	Owner	Target Date	Status
1						
2						
3						
4						
5						
6						

12. QA Sign-Off

Role	Name	Signature	Date

Annex 12: Business process documentation and re-engineering template

Process Name:	
Process Purpose:	
Process Scope:	
Process Input/Output;	
Process linkage /hand-offs in value chain/ External	
Integration with external systems	

Steps	Activity	To-be	Responsibility	Tool	Output Expected	Reports	Timelines	Remarks
1								
2								
3								
4								

Annex 13: ERP System Governance Roles and Responsibilities

a. Business Process Owners shall be responsible for:

i. Documenting as-is and to-be business processes for the functional unit in conformity with Annex 11.
ii. Defining and approving functional requirements;
iii. Approving ERP workflows, controls, and reports.
iv. Ensuring data accuracy, integrity, and completeness within their domain;
v. Approving user roles, access rights, and segregation of duties;
vi. Participating in ERP testing, acceptance, and audits.

b. The ICT function shall be responsible for:

i. ERP system availability, performance, and security;
ii. Technical architecture, integration, and infrastructure;
iii. Change and release management;
iv. User access administration and monitoring;
v. Vendor and third-party technical coordination;
vi. Ensuring compliance with ICT standards and policies.

c. Internal Audit and Assurance

a) Internal Audit shall provide independent assurance on ERP governance, controls, and compliance.
b) ERP systems shall be subject to periodic audit reviews covering access controls, segregation of duties, configuration, and transaction integrity.
c) Audit findings and recommendations shall be reviewed by the ERP Steering Committee and corrective actions tracked to closure.

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