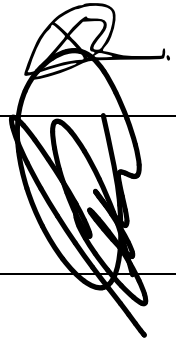
Transnet ICT Change Management Standard

Version Number	*3.0*
Effective Date	*March 2026*
Next Review Date	*2 years from the approval date*
Standard Owner	*Xolani Lukhele: GM: GICT Governance, Risk & Security*
Signature	
Standard Sponsor	*Pandelani Munyai: Chief Information Officer*
Signature	
Date Approved	25 March 2026

Recommended by Standard Owner and Standard Sponsor:

I hereby acknowledge that a search has been conducted and that the Standard is not duplicated or in conflict with any other Transnet Standards.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Owner	Xolani Lukhele	GM: Group ICT Governance Risk & Security		20/03/2026	Xolani.Lukhele@transnet.net	066 195 3363
Sponsor	Pandelani Munyai	Chief Information Officer		20/03/2026	Pandelani.Munyai@transnet.net	011 308 3071

Final Approval

ICT Architecture Review Council

25 March 2026

Date Approved

Summary of Version Control

Version Number	Effective Date	Summary of Changes
1.0	April 2014	*Approved version*
1.1	April 2019	*Updated owner and sponsor with no changes to the contents of the Change Management Standard.*
2.0	February 2023	• *Updated the Standard review date, owner and sponsor information.* • *Updated the numbering for each paragraph per section for ease of reference.* • *No material changes to the content were required during the review process from any of the operating divisions.* • *Section 5.1.14 Updated "Where feasible, testing should be done in a QA environment and documented in relevant application standard operating procedure (SOP)."* • *Section 5.2.1 Aligned to ITIL definitions for Standard, Normal and Emergency changes.* • *Section 5.3 Updated emergency changes statement.* • *Added section 5.9 Post Implementation Review of Changes.* • *Section 6 Updated Roles & Responsibilities.* • *Section 8 Added exclusions for environments that do not have a QA environment for testing.*
3.0	February 2026	• *No material changes to the contents of the standard.* • *Changed Standard owner to GM: Governance, Risk & Security.* • *The word "will" was identified in some statements as too soft and ambiguous and then replaced with "should" or "must".* • *Definitions have been moved from Appendix A into Section 3 to align with the same structure used in other Standards.* • *Added new section 5.3 including the list of CAB approved Pre-Authorised Changes.* • *Added new section 5.4 for urgent changes.* • *Section 10: Updated for OD ISO to monitor and report non-compliance to ISGRC committee.* • *Section 11: Updated non-compliance with the same statement used in all other ICT Standards.*

Table of Contents

1. BACKGROUND

Change Management's (CM) function is to ensure that modifications to the Transnet ICT environment are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner to minimise the risk of negative impact of changes to Transnet.

This standard governs changes made to all Transnet ICT Services, Service Components (SC) and Configuration Items (CIs). This includes but is not limited to:

- Host systems, including rebooting of servers.
- Environmental components, power systems, fire suppression systems within Data centres.
- All hardware components.
- Software elements including application and databases systems.
- Network components including physical cabling.
- Security devices.
- Documentation including policies, procedures, service catalogues, and system documentation.

2. PURPOSE

This Standard establishes the principles and practices for ICT Change Management within Transnet. How these principles and practices are implemented is set out within a separate, but supporting, Standard Operating Procedures (SOP) document.

3. DEFINITIONS

For ease of reference words, expressions and abbreviations used in the standard are defined below:

CAB: The Change Advisory Board delivers support to a change management team by approving requested changes and assisting in the assessment and prioritization of changes. This body is generally made up of IT and Business representatives that include: a change manager, user managers and groups, and technical experts.

CI: Configurations Items is a component that needs to be managed to deliver an IT Service.

CM: Change Management is a process that ensures standardized methods and procedures are used for efficient and prompt handling of all changes, to minimize the impact of change-related incidents upon service quality and consequently improve the day-to-day operations of the organization.

Bulk/Large scale Implementation: A roll out of a pre-authorised change that affects multiple systems, sites, or a large number (>10% of total population) of endpoints/users in a single execution window.

CMDB: Configuration Management Database is a data repository that acts as a data warehouse or inventory for information technology (IT) installations. It holds data relating to a collection of IT assets (commonly referred to as configuration items (CI)), as well as to descriptive relationships between such assets.

ECAB: Emergency Change Advisory Board is sub-set of the Change Advisory Board who makes decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called and depends on the nature of the Emergency Change.

ICT: Information and Communications Technology is another/extensional term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware and storage.

KPI: Key Performance Indicators is a measurable value that demonstrates how effectively a company is achieving key business objectives. Organizations use KPIs to evaluate their success at reaching targets.

OD (Operating Division): Transnet has the following: Operating Divisions namely TFR, TRIM, TPL, TPT, TNPA, TE, TP and TCC.

PIR: Post Implementation Review takes place after a Change has been implemented. It determines if the Change and its implementation Project were successful and identifies opportunities for improvement.

RCA: Root Cause Analysis is the underlying or original cause of an Incident or Problem. is a method of problem solving used for identifying the causes of faults or problems.

RFC: Request for Change it is a call logged or form that is completed which states what needs to be accomplished but leaves out how the change should be carried out.

SC: Service Components is a means of delivering value to customers by facilitating outcomes customers want to achieve, but without the ownership of specific costs and risks.

SOP: Standard Operating Procedure is a set of written instructions that document a routine activity that is to be followed by members of an organization.

4. SCOPE

4.1 ACTIVITIES

4.1.1 Change Management's key activities include ensuring that all changes to all environments are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed. Change Management is also responsible for reporting on the effectiveness of the process to senior management and identifying improvements that can be made and ensuring that the Change Management process is auditable and key risks have been identified and mitigated against.

4.2 AUDIENCE

4.2.1 ICT staff whose role(s) includes:

- Making changes to existing ICT Services, Service Components (SC) and Configuration Items (CIs).
- Delivering and supporting Services.
- Supporting deployed Services.
- Representing ICT to the Business.
- Any other responsibilities where awareness of the Standard is necessary.

4.2.2 Business personnel:

- Represent Business's interests as the recipient of deployed Services.

4.3 IT SERVICES

4.3.1 This Standard applies companywide to IT Services, including, but not limited to Transversal Services and Services delivered by an Operating Division (OD) to itself or other ODs.

4.4 ACTIVITIES OUT OF SCOPE

4.4.1 The scope of Change Management covers changes to Services and Configuration Items across the entire Service Life Cycle as dictated by Configuration Management

4.4.2 Changes outside the scope of the ICT Change Management process include:

- Organisational changes.
- Changes to business operations.

- Changes at an operational level such as repair to printers or other routine service components.

5. STANDARD STATEMENTS

5.1 GENERAL

5.1.1 Transnet adopted a common Change Management Process for handling and controlling changes across all Operating Divisions.

5.1.2 Change Management Process activities should be documented in a Procedures document.

- The Process and their activities should conform to ITIL and COBIT best practice, allowing for differences to enable customisation to Transnet's environment.
- Appropriate customisation to the common Change Management Process activities is permitted.

5.1.3 All Changes should follow the Change Management Process. This includes those for key Service Providers of IT Services.

5.1.4 Change Management should manage all Changes in such a way to minimise Business impact.

5.1.5 Change Management records should be audited to ensure that the information in them is accurate and complete.

5.1.6 Change Management should identify improvement opportunities and include them in the Continual Service Improvement (CSI) register.

5.1.7 Change Management should define relevant process Key Performance Indicators (KPIs), and track and report on them to ICT Management.

5.1.8 Management should ensure that sufficient resources are allocated to execute Change Management effectively and efficiently.

5.1.9 All Requests for Changes should be recorded and managed in an Information Technology Service Management (ITSM) Tool.

5.1.10 All Change records should be updated with relevant and complete information so as to record a full history. This should include, but not be limited to:

- Request for Change form.
- Risk Assessment of the change.
- A Test Plan.

- Implementation Plan.
- A Back-out Plan.
- Communication Plan.
- Report from Incident Management.
- Report from Problem Management.
- Post Implementation review report.

5.1.11 All submitted Requests for Change should be evaluated for completeness by the Change Manager.

5.1.12 Incomplete forms must **not** be submitted to the Change Advisory Board (CAB) for approval.

5.1.13 The Change Advisory Board (CAB) will authorise a Request for Change (RFC) based upon the risk assessment, service levels and provided there is a business justification for the change.

5.1.14 Where feasible, testing should be done in a QA environment and documented in relevant application standard operating procedure (SOP).

5.1.15 All Changes to existing Configuration Items (CIs) that are not yet in the Configuration Management Database (CMDB), should be added/updated to the CMDB.

5.1.16 Some incidents may or not may not be related to a Change, but where a Change has caused an incident then the Change Manager should facilitate a review meeting and a report should be generated and fed back to the Change Advisory Board. (Also refer to section 5.8 Root Cause Analysis)

5.2 CHANGE TYPES:

A change is the addition, modification or removal of any authorized, planned, or supported service or service component that could have an effect on ICT services.

5.2.1 Changes are categorised into three types:

a. **Standard Change (Preauthorised):**

ls a change that is pre-authorised by CAB, repetitive, low-risk and well tested. These changes would include operational maintenance type changes and management should have an accepted and established procedure for these changes.

b. **Normal Change:**

Is a change raised by a request from the initiator or the individual or organisational group that should go through assessment, authorisation and CAB approval before it can be implemented.

c. Urgent Change:

An Urgent Change is a change that must be implemented faster than the timelines of a Normal Change. But does not qualify as an Emergency Change. These changes address situations where delay would cause service degradation, regulatory non-compliance, operational disruption, or increased business risk, but where the impact is not immediately critical.

Urgent Changes still require assessment, authorisation, and documented approval, but follow a shortened, fast-tracked review and CAB decision process.

d. Emergency Change:

Is a Change that must be introduced as soon as possible as the result of a critical event. This event must have a significant impact on ICT services. Details are often captured at a later date.

5.3 PRE-AUTHORISED CHANGES

Pre-authorised changes are low-risk and repeatable activities approved in advance by the CAB. While these changes do not require individual CAB approval for each execution, any large-scale, bulk, or infrastructure-wide implementation of pre-authorised changes must be reported to the CAB for noting prior to execution. This ensures visibility, coordinated scheduling, and proactive management of aggregated risk.

The following is a list of CAB-approved pre-authorised (standard) changes:

5.3.1 **Identity and Access Management:**

- Monthly or regular user account terminations (e.g., leavers).

- Disabling of dormant or inactive user accounts.
- User account unlocking following lockouts.
- Password resets executed through approved processes.
- Group membership amendments aligned to approved role-based access requests.

5.3.2 **Active Directory and Directory Services**

- Creation of standard user and service accounts.
- Routine Organisational Unit (OU) management activities.
- Enforcement of existing password and directory security policies.

5.3.3 **Endpoint and User Device Management**

- Standard device join and removal from domain or MDM platforms.
- Routine endpoint security agent installations or updates.
- Endpoint quarantine or isolation for security remediation purposes.

5.3.4 **Security Operations**

- Blocking malicious domains, IP addresses, or URLs based on threat intelligence.
- Routine email and firewall rule clean-up (disable or remove unused rules).
- Enforcement of existing security baselines without architectural changes.
- Regular vulnerability remediation aligned to approved patch cycles.

5.3.5 **Network and Infrastructure Operations**

- Routine DNS record updates with no production impact.
- Standard VLAN or port configuration changes for end-user connectivity.
- Network access revocation for decommissioned devices.
- Log retention and archive management activities.

5.3.6 **Patch and Maintenance Activities**

- Monthly/daily operating system patching: Routine application of security patches, software updates, or antivirus signature updates.
- Standard application patching aligned to vendor recommendations.
- Firmware upgrades conducted within approved maintenance windows.

5.4 URGENT CHANGES

5.4.1 An Urgent Change is a time-sensitive change that cannot wait for the normal CAB cycle but does not meet the critical severity required for an Emergency Change. These changes address situations where delays may cause service degradation, operational disruption, or compliance risks.

5.4.2 An Urgent Change must undergo an expedited assessment to ensure that the risks, impacts, and back-out plans are clearly understood before implementation.

5.4.3 Urgent Changes must be authorised by the Change Manager and at least two CAB members, or by the CAB Chairperson (or delegate), using an accelerated approval process such as email or virtual approval.

5.4.4 Full documentation must be submitted to the CAB at the next scheduled CAB meeting for review.

5.4.5 An RFC for the Urgent Change must be created within a reasonable timeframe and no later than 24 hours before implementation, unless circumstances require immediate action.

5.5 EMERGENCY CHANGES

5.5.1 Each situation is different and as much consideration as possible should be given to the possible consequences of attempting this type of change.

5.5.2 An emergency change should be designed carefully and tested before use if possible, or the impact of the emergency change may be greater than that of the original Incident.

5.5.3 Emergency Changes must be authorised by the Emergency Change Advisory Board (ECAB). Full documentation must be submitted to the CAB upon abatement of the crisis.

5.5.4 An RFC for the Emergency Change must be created within a reasonably timeframe within 24 hours after the change.

5.6 CHANGE ADVISORY BOARD (CAB)

5.6.1 The Change Advisory Board (CAB) reviews all RFCs submitted and determine whether or not they should be implemented. In addition, it may determine that certain changes are altered before implementing.

5.6.2 The CAB should meet weekly except during change freeze periods. The Change Manager should provide an agenda of newly submitted items and a change status schedule. The purpose of this meeting is to:

- Bring all required parties together to assess the feasibility of implementing the change and provide status.

- To review the status of all open changes and schedule for the current and upcoming weeks.
- Discuss high impact changes.
- Approve or decline each change.

5.6.3 Attendees of these weekly meetings should include the following representatives, for both Transnet Group and the various Operating Divisions (ODs):

- Change Manager.
- All Operating Divisions representatives.
- Service provider/vendor representatives.
- IT Security representative.
- Service Desk representative.

5.7 EMERGENCY CHANGE ADVISORY BOARD (ECAB)

5.7.1 We appreciate that due to the nature of these types of changes that it is not very practical to either wait for group of advisory board members to gather or to seek approval for a change to be made. This is made especially difficult for out of hour's incidents that require immediate or quick changes to be made to restore a service. In these circumstances, the Change Manager, GM Enterprise Service Delivery and representatives from the ODs affected by the Change, have the authority to approve a change.

5.7.2 The change request form should still be filled in, even if it is retrospectively.

5.8 CHANGE FREEZE PERIODS

5.8.1 At certain critical times of the year, it may be necessary to impose a non-essential change freeze period. This can be partial or full, meaning that it applies to all services or only some.

5.8.2 During this time only changes deemed essential to either the running of or fixing of a problem with a particular service should be considered for approval and implementation.

5.8.3 Approvals need to be obtained from the assigned role/roles as per the requirements of section 5.4.

5.8.4 The dates of any change freeze should be communicated well in advance to enabled teams to plan and work around them. The communication will also advise on how to obtain approval for essential changes during this time.

5.9 RESCHEDULING OR CANCELLATION OF A CHANGE

5.9.1 If for any reason a CAB-approved change has to cancelled or postpone, then the Change Manager has to be informed.

5.9.2 If the Change need to be performed at a later date, then a new RFC should be submitted.

5.10 ROOT CAUSE ANALYSIS

5.10.1 A root cause analysis for a failed change should include:

- Basic information about the change e.g., Change reference number, implementation date and change description.
- Business impact as a result of the failed change.
- Root cause of the failed change.
- Preventative measures.

5.11 POST IMPLEMENTATION REVIEW OF CHANGES

5.11.1 After any change has been implemented, the person who is responsible for implementing the Change should perform a Post Implementation review of the Change.

5.11.2 Post Implementation Review feedback should be provided to CAB and included in the CAB meeting minutes.

5.12 CHANGE RECORD CLOSURE

5.12.1 Before a Change record is Closed, the following quality assurance should be done:

- Verification that the Change was implemented as planned.
- The change should be closed with appropriate closure category.
- Failed changes should be closed and resubmitted as a new change.

5.13 UNAUTHORISED CHANGES

5.13.1 Unauthorised Changes are a serious breach of this standard and an unacceptable risk to Transnet. If unauthorised changes are detected, the CAB should sanction an investigation to determine the impact of the unauthorised Changes and what actions need to be taken.

6. ROLES AND RESPONSIBILITIES

Responsible:	Service Delivery Manager
Accountable:	GM: Enterprise Technology & PMO Services
Monitoring:	ICT Operations Council
Standard Owner:	GM: GICT Governance, Risk & Security
Standard Sponsor:	Chief Information Officer

7. RELATED INFORMATION AND REFERENCE

This Standard should be read in conjunction with the following supporting guidelines:

7.1 INTERNAL DOCUMENTS

- ICT Governance Policy
- Transnet Information Security Policy
- ICT Vendor Management Standard
- ICT Cloud Standard

7.2 EXTERNAL DOCUMENTS

- ISO/IEC 27001 – Information Security Management
- ISO/IEC 27002 – Information Security Controls
- ISO/IEC 27005 – Information Security Risk Management
- ITIL (Information Technology Infrastructure Library)
- COBIT 5

8. EXCLUSIONS

The following environments do not have a Quality and Assurance (QA) or test environment. Changes to these environments will be implemented directly in the Production Environment for testing in a controlled manner with a rollback plan:

Example:

- Cloud Security Services (e.g., AAD, MDE, Mimecast, Cloudflare)
- Active Directory
- Firewall
- VMWare
- Network Devices
- Printers

A full list of Cloud Security Services can be found on the Transnet Intranet. Waivers - All Documents (path: SharePoint>Policies & Procedures>ICT Standards>2.Waivers)

9. REQUEST TO DEVIATE FROM STANDARD

In cases where material and compelling circumstances merit deviation(s) from particular provision(s) of this Standard, written submissions shall be sent to the GICT GM Governance, Risk and Security, who shall have full authority to grant such request, in whole or in part, or to refuse same.

10. COMPLIANCE MONITORING

Compliance monitoring should be performed by the Operating Division Information Security Officer (OD ISO). Any non-compliance with this Standard that requires further action should be reported to the ISGRC Committee for escalation, oversight, and remediation.

11. NON-COMPLIANCE

Each employee is responsible for complying with the requirements of this standard. Any violation may result in one or more of the following actions:

- Restriction or removal of access to some or all Transnet systems for employees or third parties.
- Corrective or disciplinary action in accordance with the Transnet Disciplinary Code and Procedures and any other applicable policies.
- Legal action, including civil or criminal proceedings, where permitted under applicable law.
- Restitution, where the violator may be required to compensate Transnet for any loss or misuse of services.
- Termination or cancellation of contracts with third-party service providers.