TIDEWELL FINANCIAL

Technology Governance Program

IT Change Management Standard

Standard No. TGP-STD-310

Version 2.0 | Effective June 1, 2026

Portfolio writing sample by David Parker Jr. Tidewell Financial is a fictional organization; all names, document numbers, and requirements in this document are invented for illustration.

Contents

1 Purpose
2 Scope and Authority
3 Adherence Reporting
4 Compliance
5 Exceptions and Risk Acceptance
6 References
7 Standard
    7.1 Change Classification
    7.2 Change Request Requirements
    7.3 Review and Approval
    7.4 Implementation
    7.5 Emergency Changes
    7.6 Post-Implementation Review
    7.7 Monitoring and Reporting
8 RACI Matrix
9 Terms and Definitions
10 Reviewers and Approvers
11 Revision History

1 Purpose

This Standard establishes the minimum requirements for recording, assessing, approving, carrying out, and reviewing changes to Tidewell Financial's production technology environment. Its goal is to let the organization change its systems quickly while limiting service disruptions, security exposure, and unauthorized modifications.

2 Scope and Authority

This Standard is issued under the authority of the *Technology Governance Policy (TGP-POL-100)*. It applies to all employees, contractors, and third parties who design, build, configure, operate, or retire IT assets that support Tidewell Financial production services, including services hosted by third parties on Tidewell Financial's behalf.

Out of scope are changes to non-production environments that cannot affect production, and changes to end-user devices managed under the Endpoint Management Standard (TGP-STD-340).

3 Adherence Reporting

The Standard owner must be able to show that the requirements in Section 7 are being met. The Change Management Office (CMO) will test the evidence listed in Figure 1 each quarter and report the results to the Technology Governance Committee.

Figure 1. Adherence evidence

Requirement area	Evidence tested
Change classification (7.1)	Sample of closed change records shows each change was classified, and every Standard change used an approved template.
Change request content (7.2)	Sample of Normal change records contains all required fields, including test evidence and a backout plan.
Review and approval (7.3)	CAB minutes and approval records show that Medium- and High-risk changes were approved before implementation, and that no change was approved by its own implementer.
Emergency changes (7.5)	Each emergency change has a complete record within two business days and was reviewed at the next CAB meeting.
Post-implementation review (7.6)	A PIR exists for every failed, emergency, and High-risk change in the period.
Monitoring and reporting (7.7)	Monthly change metrics report was delivered to the Technology Governance Committee.

4 Compliance

All new IT assets must meet this Standard before they are placed into production. Existing IT assets must also comply. Where an existing asset or process does not comply, the Service Owner must submit a remediation plan to the CMO within 30 days of the gap being identified. The plan must state the actions, owners, and target dates needed to reach compliance.

5 Exceptions and Risk Acceptance

When a requirement cannot be met because of a technical limitation or a business constraint, the Service Owner must request an exception through the Technology Risk exception process before the non-compliant activity begins. Each request must describe:

- the requirement that cannot be met and why;
- the compensating controls that will reduce the resulting risk;
- the plan and target date for reaching compliance.

Exceptions are granted for no more than 12 months. The residual risk must be accepted in writing by a Senior Director or above who is accountable for the affected service.

6 References

This Standard must be read and maintained in conjunction with the following documents.

Tidewell Financial documents

- TGP-POL-100 Technology Governance Policy
- TGP-STD-320 Incident Management Standard
- TGP-STD-330 Configuration Management Standard
- TGP-STD-340 Endpoint Management Standard

External frameworks

- ITIL 4, Change Enablement practice
- NIST SP 800-53 Rev. 5, control CM-3 (Configuration Change Control)

7 Standard

7.1 Change Classification

7.1.1 Every change to a production IT asset must be recorded in the enterprise change management system before work begins, except as permitted for emergency changes in Section 7.5.

7.1.2 The Change Owner must classify each change as Standard, Normal, or Emergency.

7.1.3 Standard changes must follow a template approved by the CAB. The CMO must review the catalog of Standard change templates at least annually and retire any template whose changes have failed more than twice in the preceding 12 months.

7.1.4 The Change Owner must assign each Normal change a risk rating of Low, Medium, or High using the risk assessment questions in the change management system.

7.2 Change Request Requirements

7.2.1 Each Normal change request must include, at a minimum:

- a description of the change and its business justification;
- the configuration items (CIs) and services affected;
- the risk rating and the answers that produced it;

- the implementation plan and requested implementation window;
- evidence that the change was tested in a non-production environment;
- a backout plan that can be completed within the approved window.

7.2.2 Where a change affects customer-facing services, the request must also include a communication plan for affected business units.

7.3 Review and Approval

7.3.1 Low-risk Normal changes must be approved by the Service Owner and peer-reviewed by a technically qualified person other than the implementer.

7.3.2 Medium- and High-risk Normal changes must be approved by the CAB before implementation.

7.3.3 No person may approve a change that they will implement.

7.3.4 The CAB must meet at least weekly. A quorum requires a CMO representative and representatives from at least three technology functions.

7.4 Implementation

7.4.1 Changes must be implemented only within the approved window. A change that cannot be completed within its window must be backed out unless the Service Owner approves continuing.

7.4.2 Non-emergency changes must not be implemented during a freeze period unless approved in advance by the Chief Technology Officer or a delegate.

7.4.3 The Change Owner must record the outcome of each change (successful, successful with issues, backed out, or failed) within one business day of implementation.

7.5 Emergency Changes

7.5.1 Emergency changes may be used only to restore a service during an active incident or to address an active or imminent security threat.

7.5.2 Each emergency change must be approved before implementation by the on-call technology manager and the Service Owner or their delegate. Verbal approval is acceptable if it is recorded in the change record.

7.5.3 A complete change record must be entered within two business days of implementation, and the change must be reviewed at the next CAB meeting.

7.6 Post-Implementation Review

7.6.1 A post-implementation review (PIR) must be completed within 10 business days for every failed change, every emergency change, and every High-risk change.

7.6.2 Each PIR must identify the root cause of any failure and any corrective actions, with owners and due dates. Corrective actions must be tracked to closure by the CMO.

7.7 Monitoring and Reporting

7.7.1 The CMO must report the following metrics to the Technology Governance Committee each month: change success rate, emergency change rate, number of changes implemented without approval, and number of overdue PIRs.

7.7.2 Any change found to have been implemented without approval must be raised as a security incident under the Incident Management Standard (TGP-STD-320).

8 RACI Matrix

Figure 2 identifies who is Responsible, Accountable, Consulted, and Informed for each section of this Standard.

Figure 2. Roles and responsibilities

Section	Change Owner	Service Owner	CAB	Change Mgmt Office	Technology Risk
7.1 Change Classification	R	A	I	C	I
7.2 Change Request Requirements	R	A	I	C	I
7.3 Review and Approval	C	R	A	R	C
7.4 Implementation	R	A	I	I	I
7.5 Emergency Changes	R	A	C	R	I
7.6 Post-Implementation Review	R	C	A	R	I
7.7 Monitoring and Reporting	I	I	I	A/R	C

R = Responsible A = Accountable C = Consulted I = Informed

9 Terms and Definitions

Term	Definition
Change	The addition, modification, or removal of anything that could affect a production IT service, including hardware, software, configuration, and documentation.
Change Advisory Board (CAB)	The group that assesses, prioritizes, and authorizes Medium- and High-risk Normal changes.
Change Owner	The person accountable for planning and carrying out a specific change.
Configuration Item (CI)	Any component that must be managed to deliver an IT service and is recorded in the configuration management database.
Emergency change	A change that must be made as soon as possible to restore service or to address an active security threat.
Freeze period	A defined period during which non-emergency changes to production are not permitted.

Term	Definition
Service Owner	The person accountable for the delivery and performance of a specific IT service.
Standard change	A pre-authorized, low-risk change that is performed often and follows an approved, documented procedure.

10 Reviewers and Approvers

Role	Title
Standard Owner	Director, IT Service Management
Reviewer	Manager, Change Management Office
Reviewer	Senior Manager, Technology Risk
Approver	Chief Technology Officer

11 Revision History

Date	Version	Summary of change	Updated by	Approved by
03/14/2025	1.0	Initial release.	CMO	CTO
05/18/2026	2.0	Added Standard change template review (7.1.3), segregation of duties (7.3.3), and freeze period approval (7.4.2). Reduced emergency record deadline from five to two business days (7.5.3).	CMO	CTO