The University of Texas Rio Grande Valley™

IT Change Management

Standard and Procedures

Table of Contents

Introduction

Higher education is constantly evolving and growing, and this is particularly true in how IT supports the higher education mission. As IT organizations shift from primarily providing *technologies* to providing *services*, IT service change management is more important than ever.

Change management is a control process that helps the IT organization meet changing business needs in a timely way while stabilizing the IT services and infrastructure that need to change in order to meet those needs.

Managing change spans all IT service management (ITSM) life-cycle stages and processes. It is integral to managing the portfolio, configuration, release, incident, problem, service level management, request fulfillment, and other processes. When used consistently across the IT organization, a change management process helps accurately document the current state of IT systems and services, often helping with institutional audit requirements.

Change management develops standard methods and procedures to maximize the success of a change while minimizing impact and risk. The process promotes transparency within the IT organization, as well as with campus partners, so that everyone can be aware of changes before being impacted by them.

Defining Change

From an IT perspective, changes happen daily. In fact, changes are often a product of the work completed in IT. Was an application error reported and then resolved by implementing a patch? If so, that was a change. Did a user report a website that was inappropriately blocked by a web filter, which resulted in an update to the firewall configuration? That was also a change. Managed or not, changes occur as a result of work we accomplish—managing change is not about preventing change but rather ensuring that changes are appropriately evaluated, scheduled, and communicated to minimize the risk and impact.

A change is the addition, removal, or modification of anything that might have an impact on the delivery of an IT service. The change management process is the process used to control those changes. These include hardware (servers, routers, switches, etc.) and software (purchased or developed in house), as well as less obvious items such as documentation, policies, processes, and management tools.

Three types of changes are commonly found in higher education: standard, normal, and emergency.

- **Standard Change:** A change that is preapproved by a change authority (typically the change advisory board, or CAB—see "Roles and Responsibilities" below) and requires no additional approval to implement. Standard changes are well understood and proven (they have been implemented before successfully), are low risk, require no additional budget to implement, and have a defined trigger for when they should be implemented. Each standard change should use a change model that
  - is well documented with specific work instructions,
  - has clearly defined roles and responsibilities,
  - has established timelines (which might include a predefined change/maintenance window), and
  - has an escalation procedure.
- **Normal Change:** A change that is complex or represents significant risk or impact to the organization and is controlled through the change process. Oftentimes, the easiest way to define a normal change is that it does not fall into the emergency change or standard change categories. A typical change process for a normal change includes creating and submitting a formal proposal to make the change (often called a *request for change*, or RFC), a review of the request, approval of the request by the CAB, coordination of the change implementation, and closing the change record.
- **Emergency Change**: A change that is required to restore the normal operation of a service. Additionally, an emergency change may be required due to a security vulnerability. Break/Fix changes required within or outside normal business hours will be handled by the Service Owner following the IT Alerts procedure. The RFC for an emergency change must be submitted two business days after the change has been implemented and requires a post-change review.

IT Alerts Procedure Link:
https://utrgv.sharepoint.com/:x:/r/sites/daa/it/techservices/appdev/_layouts/15/WopiFrame.aspx?sourcedoc=%7B1f13a728-4e21-465a-bb98-4caac23955ba%7D&action=default

Roles and Responsibilities

Clearly defined change management roles are necessary to effectively carry out the practice of change management. A role does not necessarily need to be filled by one individual; a single person may assume multiple roles in the process depending on the department's size and structure. The importance of role assignment is to achieve consistency of accountability and execution.

Change Requester

The change requester submits the request for change. Generally, the change requester does the following:

- Reviews RFCs with change approver, when applicable.
- Ensures that RFCs are complete and include accurate representation of the change's priority, impact, and change window/time requirements.
- Ensures that communications pertinent to the change reach all relevant stakeholders.
- Works with the change implementer to coordinate the change.
- Closes completed changes after validation.

Change Implementer

The change implementer is the person who places the change in production. In some cases, the change implementer is the same as the change requester. The change implementer's responsibilities typically include the following:

- Oversees the overall planning, initiation, and execution of the change.
- Assigns the work for the change.
- Ensures the change has received all approvals and is scheduled in the change management system prior to implementation.
- Manages any recovery that is necessary in the event of a failed change.

Change Reviewer

The change reviewer validates that a change meets business needs; this role is often held by a key customer in the business department (e.g., registrar, HR, finance) affected by the change. Requiring that the change reviewer is a different person from the change requester and change implementer helps ensure an appropriate separation of duties that can mitigate risk for sensitive systems. The change reviewer generally does the following:

- Works to ensure that all user groups that use the product or service have

verified the change.

- Verifies the change does what it was expected to do (and only what it was expected to do) in development, testing, and production environments.

Change Approver

The change approver is responsible for reviewing the RFC and ensuring that it is technically ready for implementation. The change approver:

- Is generally the requestor's supervisor.
- Ensures the change is warranted based on a business justification.
- Is responsible for the initial approval of a change request prior to submission to the CAB.
- In the case of a failed change, ensures the change requester conducts a recovery.

Change Manager

The change manager performs the day-to-day operational and managerial tasks associated with the change management. The role is responsible for identifying opportunities for improvement and continually audits the use of the process on an operational level. Finally, the change manager is responsible for liaising with and providing reports to other service management functions. The change manager should be an influencer or a decision maker within the organization. Generally, the change manager has these responsibilities:

- Chairs and facilitates the change advisory board.
- Ensures that the CAB has evaluated all changes for compliance, appropriate planning, and communication to protect the interests of the institution.
- Schedules and attends all meetings concerning the change management process.
- Is accountable for the change approval and rejection process.
- Is accountable for the accuracy of the change schedule.
- Coordinates post change reviews as needed.
- Is responsible for reporting issues regarding the change management process and/or change management tool to the change management process owner.
- Provides input regarding change management service improvement.
- Captures and reports change management service measurement data as needed.
- Create and process violation reports as necessary

Change Management Process Owner

The person fulfilling this role has end-to-end responsibility for the way in which the change management process functions and develops. The main role of the change management process owner is to ensure that the processes are efficient, effective, and fit-for-purpose. The change management process owner works closely with other process owners to ensure integration of the disciplines and their process flows. Generally, the change management process owner:

- Is accountable for development, implementation, and communication of the change management mission and strategy in line with the mission of the institution.
- Ensures overall compliance with change management process standards and procedures.
- Is involved with development of, and subsequent agreement on, service level targets and target improvements related to the change management service.
- Captures and reports appropriate change management service measurement data.

Change Advisory Board

The CAB is the group that convenes to vet changes and to assist the change manager in the scheduling and assessment of changes. CAB members should consider both business and technical viewpoints when discussing and approving changes. Generally, members of the CAB ensure the following:

- Actively participate in scheduled meetings.
- All change requests have been submitted with sufficient information.
- Accurate risk and impact analyses have been completed and the appropriate change level is assigned for every change request.
- Proposed changes are evaluated and voted upon.
- Completed changes are reviewed.
- All failed and emergency changes undergo a post-change review.

Emergency Change Advisory Board

The Emergency Change Advisory Board (ECAB) advises the change manager in authorizing an emergency change. The ECAB typically comprises senior IT leaders and other pertinent stakeholders based on the nature of the emergency. The ECAB meets as needed in response to an emergency change.

Stakeholder

A stakeholder is a person who has an interest in an organization, project, IT service, etc.

Process

Plan the Change

When planning the change, the Requester and Change Manager are responsible for the following:

- Determining if the change is an emergency, standard, or a normal change
- Identifying the need for changes to production processes or systems
- Following the appropriate Change Management Process (Emergency, Standard, Normal)
- Determining the timeframe for the change
- Working with the appropriate people to schedule the planned change
- Identifying the individuals involved in testing the change
- Maintaining communications with stakeholders as the change progresses from inception to validation
- Assuring that approvals occur within the needed timeframe
- Verifying and documenting the outcome of the changes and rating their success

Test the Change

Every change must have a verification plan which will assure the change is made successfully. The verification plan may include pre-testing in a test environment, or alternatively breaking the change into sufficiently small increments that can be tested in off-hours using production environments for systems that do not have a test environment. The results will be documented and verified as part of the change management process.

The individual testing the change is responsible for the following:

- Developing an appropriate test plan
- Developing an appropriate verification plan
- Identifying any inadvertent consequences that might result in stability or security issues
- Verifying successful test results: resolving and re-testing any issues
- Documenting test results

- Communicating test results to the data owner
- Developing, testing and documenting a back-out plan
- Verifying back-ups beforehand when production environments are used

Approve the Change

The change request, test results and sign-off document must be presented to the appropriate approver for review of the change to be implemented.

Any exceptions to the above must be justified due to its urgency or non-negotiable due date, and reason for the exception.

Each member of the Change Advisory Board (CAB) is responsible for reviewing normal changes within the current ITSM tool. The individual must review the change to determine whether their area is affected and to ask any necessary questions of the initiator. A meeting with the Initiator and Change Advisory Board may be necessary to review the requested change. If a meeting is required, the Initiator must be present to answer any questions or address any concerns the Change Advisory Board may have.

The Change Advisory Board (CAB) should assess the risks and benefits of either making the change or not making the change. The CAB reserves the right to alter the change plan, make recommendations and/or send it back for revisions if the change proposal is unacceptable or requires additional work.

Implement the Change

The Change Advisory Board authorizes the change to be implemented. Only changes that have been approved may be implemented in a production environment.

The implementation team is responsible for the following:

- Obtaining authorization from the appropriate Change Manager to migrate the change
- Ensuring adequate staff is available to migrate the change
- Communicating the migrated change to the appropriate Change Manager
- Migrating successfully tested changes to the production environment

Validate the Change

After implementation of a change, validation of the change must occur in order to verify if the change was successful. If validation fails, the change must be reverted using its back out plan.

Document the Change

All change requests must be formally documented, classified, and prioritized in the current ITSM tool to ensure they are planned for accordingly.

All those involved in the Change Management Process are responsible for reviewing the documented changes for correctness, completeness, and adherence to standards and procedures.

The Change Request Form in the current ITSM tool contains detailed information about the change and is required for changes submitted to the Change Advisory Board.

All change requests must be maintained in the current ITSM tool for awareness that a change is being or has been implemented.

Change control documentations such as diagrams, schematics, processes must be updated to reflect the current state after the change (i.e., all documentation must be updated before the change request can be closed). An index must be maintained of revision levels to identify current official revision.

Close the Change

All changes must be closed by the requestor within a six-month period and must indicate one of the following closing codes:

- Change Successful
- Change Successful but had a few issues
- Change Successful but exceeded the planned end time
- Change Backed out
- Change Cancelled – it was never started

Standard and Normal changes that were successful with few issues or backed out will need a post-change review by the change manager prior to closing. All emergency changes will require a post-change review by the change manager prior to closing.

Change Management Activities

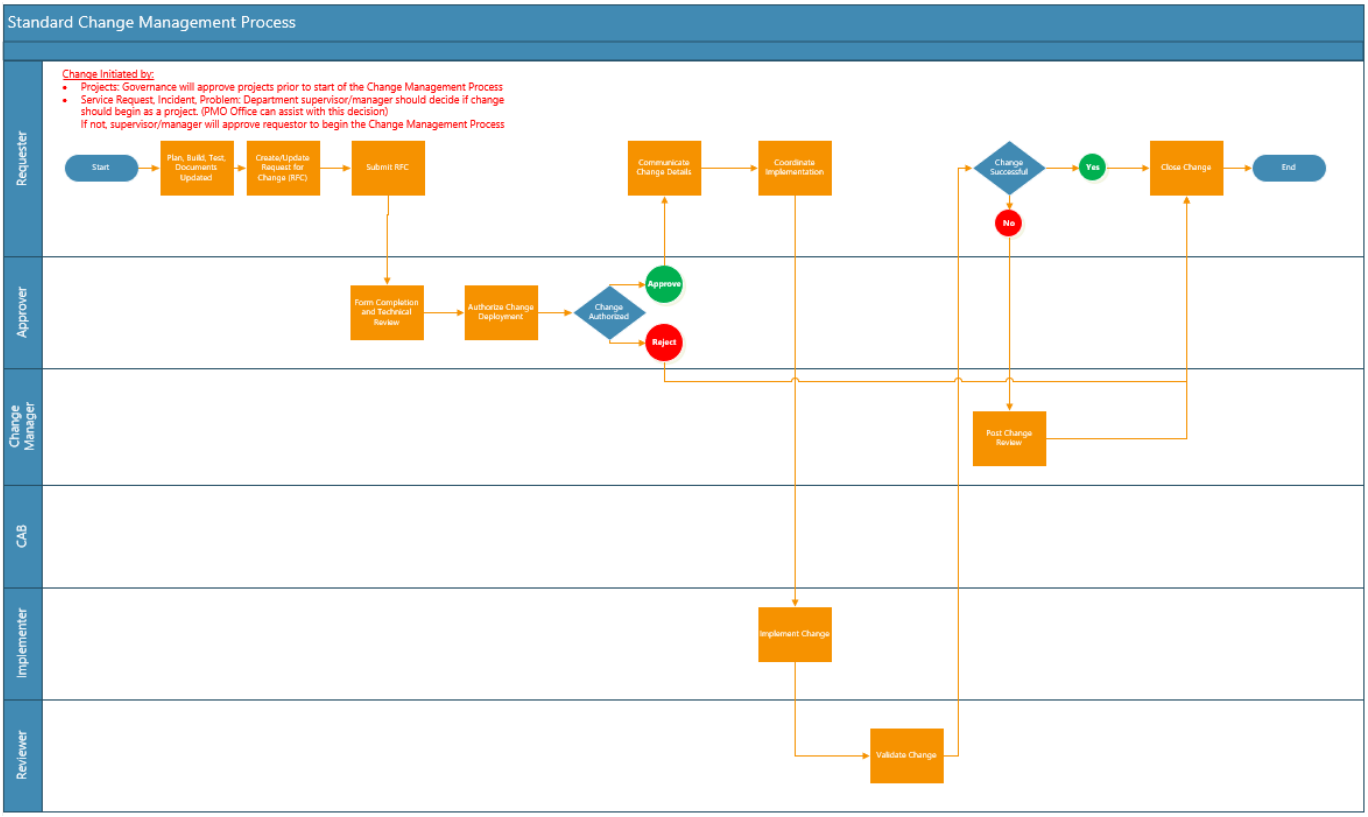
Depending on the number of changes and the size of the institution, the number of people involved, and the documentation required will vary.

Table 1. Change management activities

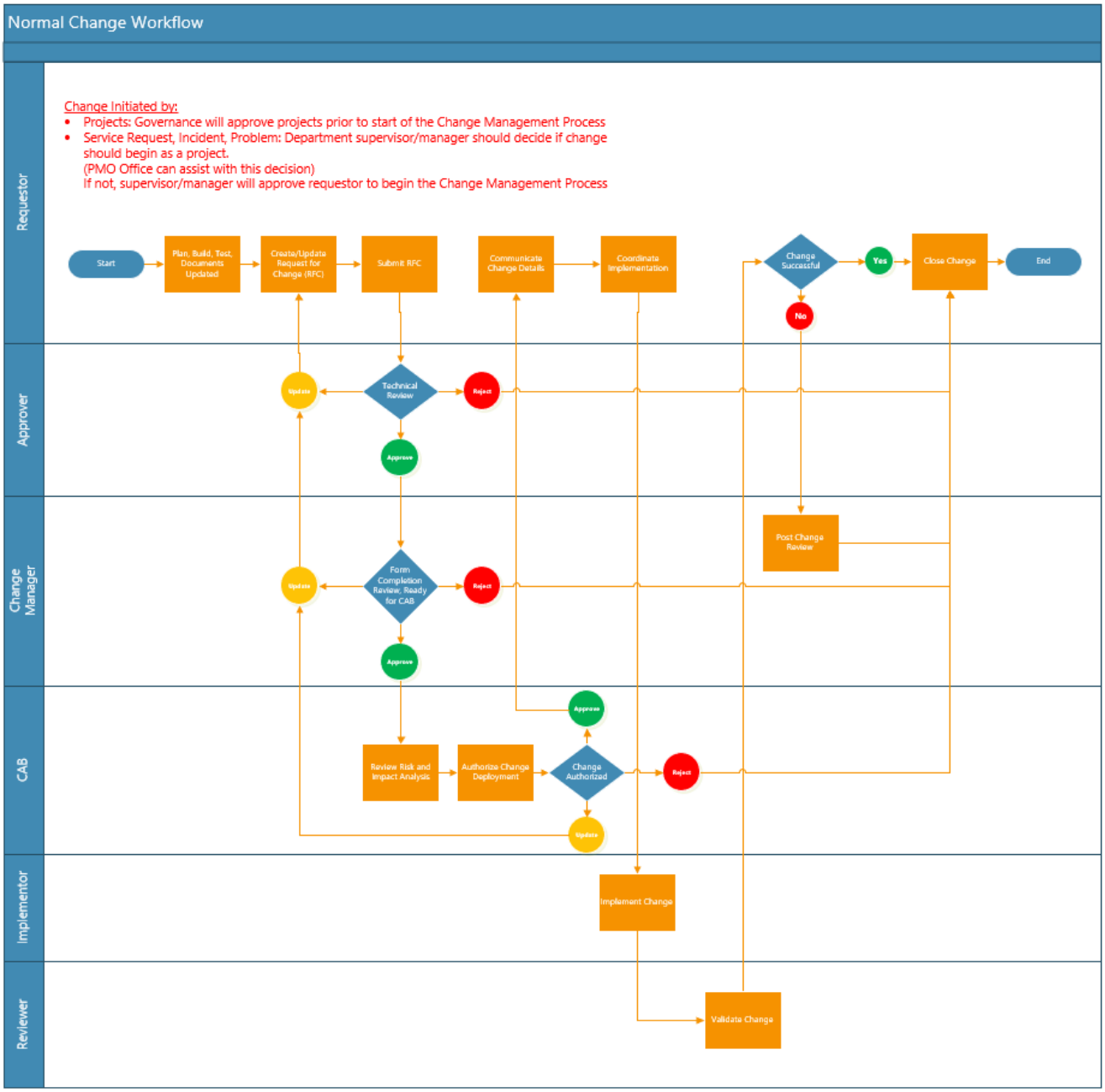
Activity	Description (Procedures)
1.1 Create Request for Change (RFC)	The change requester must have supervisor/manager prior approval to plan, build and test a change. Once completed, the change requestor follows the change management work instructions to create the RFC..
1.2 Submit RFC	The RFC is submitted for approval using a predefined tool or system.
1.3 Review RFC for Completeness	The RFC is reviewed for completeness. Based on type of change, additional reviews might be performed, such as peer review, management review, or change manager review. At this stage the RFC may be returned to the change requester if it is not complete.
1.4 Review Risk and Impact Analysis	The risk and impact analysis of the change is reviewed by the approval authority. (See "Risk and Impact" below.)
1.5 Authorize Change Deployment	The approval authority validates that there are no conflicts in the published change schedule. The change is authorized for deployment and sent to requestor. If the RFC is rejected, it is returned to the requester with an explanation.
1.6 Communicate Change Details	The change requester communicates the change details to the appropriate stakeholders.
1.7 Coordinate Change Implementation	The change implementer defines the steps for the change implementation, coordinates the work, and executes the change. If the change fails, the change implementer will implement the back-out plan to restore the service to the prior known working state.
1.8 Review Change Outcomes	Upon execution of the change, the change implementer and change requester validate that the change produced the intended outcomes. Other stakeholders may be involved in this step to ensure the change was successful.
1.9 Close RFC	The change requester closes the change.

Workflows

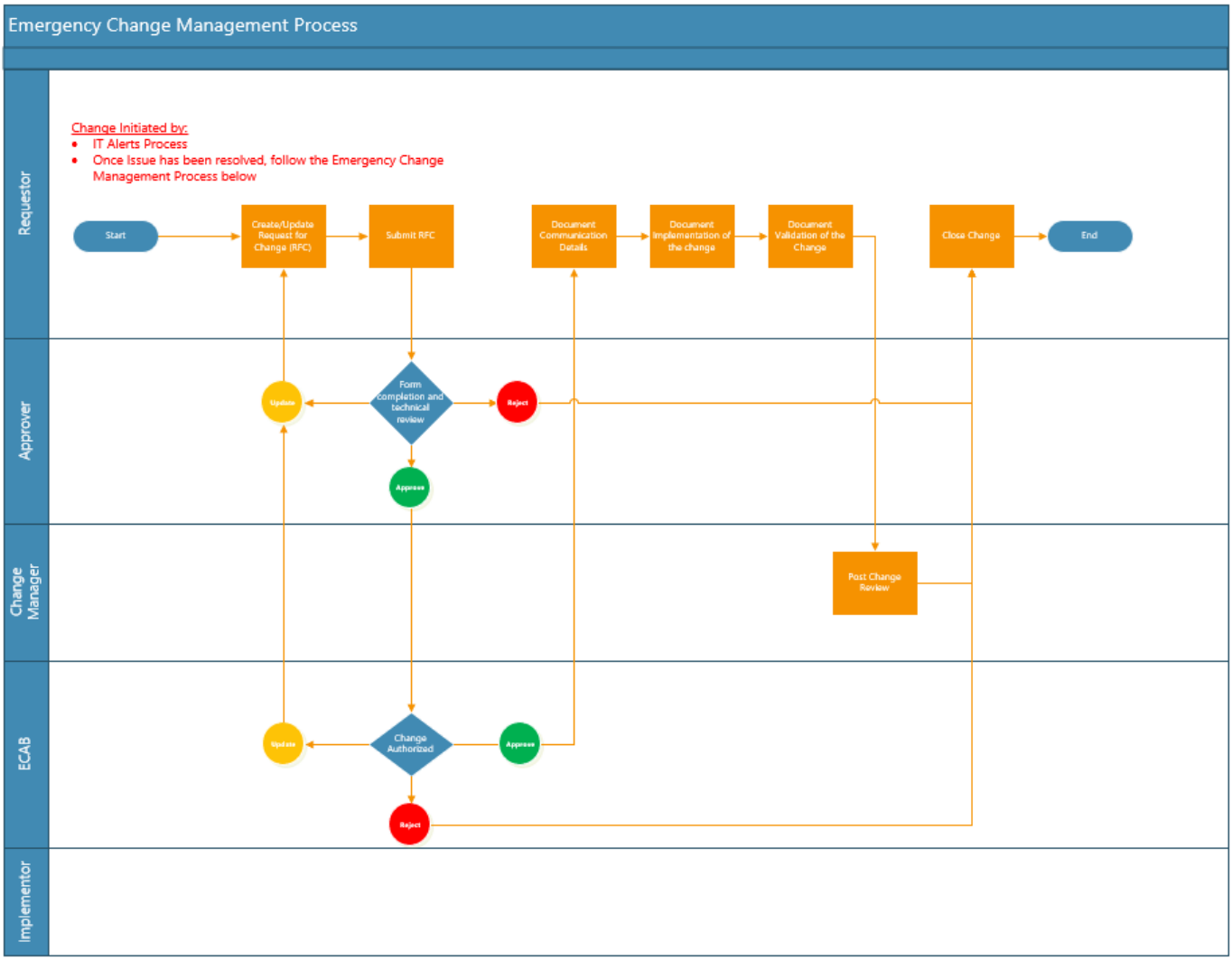
Standard Change



Normal Change



Emergency Change



Violations

Violations to UTS 165 and the UTRGV Change Management Policy may result in disciplinary action. When a violation is identified, the Change Manager will create a Violation Report including details of the violation. The violation will be submitted to the supervisor and Chief Information Officer (CIO). The Change Manager will maintain a log of violations and the amount of times an employee has violated the policy. First and second violations will be considered warnings. Upon the third violation, a corrective action plan and retraining plan will be developed with the employee and their supervisor.

Review

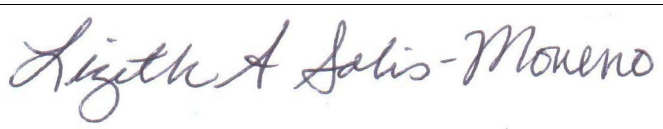
The Chief Information Officer shall review this standard annually.

This document has been adopted from EDUCAUSE

Review History

Date	Version	Description	Author
12-Aug-2019	2.0	Adopted Educause Change Management document with revisions including violations section.	Lizeth Solis-Moreno

Approvals

Approver name	Department/Role	Signature	Date
Lizeth Solis-Moreno	IT Change Management Coordinator		9/16/2019
Isai Ramirez	IT Governance & Services		9/16/2019
Dr. Jeffrey Graham	Chief Information Officer	Jeffrey A Graham	9/25/29