Change Management Process

Last Updated: 1/29/2026

CONTENTS

OVERVIEW

SUMMARY

The Change Management process was established to:

- facilitate the exchange of information between units of C&IT and between C&IT and the university community
- facilitate the stability of enterprise-wide systems by minimizing risk and disruptions
- have a record of system changes that can assist in problem resolution

This document details the Change Management process policy and its procedures.

SCOPE AND MANAGED CHANGE DEFINITION

A managed change is any action associated with a C&IT configuration item (e.g., application, service, or server) that meets the following criteria:

- There is a conceivable risk of the change causing any type of observable disruption (e.g., inability to perform work, poor system performance, risk of data loss, etc...)
- The configuration item is currently being used by at least one customer

Any change that meets the definition of a managed change should be handled by the change management process. Any other changes that do not meet these criteria do not need to be handled by this process.

OVERVIEW

Configuration items (CIs) refer to any type of asset (e.g., application, server, equipment, etc…) that may be the subject of a change. CIs allow for greater flexibility and control over the change management process by allowing the unique needs of any given CI to be considered throughout the change management process. Any CI that is affected by a change should have its properties clearly defined early in the change management process.

CI CHANGE PROPERTIES

All CIs should have the following properties defined and documented:

- Name
- Normal Approver(s)
- Impact Change Window

It is recommended that CIs and their parameters should be as broad as possible. For example, it is recommended that parameters be defined at a high-level like "HR Applications," if possible, rather than each application in HR (e.g., "EPAF", "Open Enrollment", "Payroll", "WSAM", etc...).   In this example, if all of the applications have the same change properties (i.e., approvers, change windows, notification lists, etc.), then they should likely all be grouped as one CI. If an application/server/service has specific properties that vary, then it may require a separate CI.

Similarly, it is recommended that the change window be inclusive of all hours that an approver is authorized to consider for the impact change windows. The expectation is that approver(s) will consider the unique needs and risks of any given change and will be empowered to approve implementation times that best balance all considerations. Change windows should only limit hours in cases where the approver does not have the authority to implement a change at a given time and where value is added by escalating the approval decision to the Change Advisory Board (CAB).

Please note that CIs do not need to be limited to the production environment. Changes in a test environment may meet the definition of a managed change if they have the potential to be disruptive to users (e.g., functional leads and developers). In these cases, it would be appropriate to define a test system as a CI.

When determining if a change has a low, medium or high impact, the Change Owner can use the following attributes (and any other relevant factors) to select the appropriate impact level for a particular change:

	Availability of CI	Performance of CI	Ease of Back Out Plan
High	Known outage/Potential for extended outage	Up but unstable	Very slow restore, i.e. from back up

Medium	Potential for short outage	Slow but usable	Multi-step restore process
Low	Very low risk of outage	Little impact	Quick one step roll back

Name	Academica
Normal Approver	Chuck Plater
Escalation Approver	CAB
Impact Change Window	Thu 6am-8am, Sun 2am-8am
Name	Wireless Controllers
Normal Approver	Matthew Lessins
Escalation Approver	CAB
Impact Change Window	Sun, 2AM to 8AM

CHANGE TYPES

OVERVIEW

SUMMARY OF CHANGE TYPES

The change management process defines the criteria and process flow for the following three distinct change types:

1. Normal Change
2. Emergency Change
3. Pre-Approved Change

The appropriate change types can be summarized using the table below; more detail appears in the subsequent decision chart:

	Is the CI operating normally?	Has the change been pre-approved and has its change process been documented?
Normal Change	Yes	No
Emergency(Escalation) Change	No	No
Pre-Approved Change	Yes	Yes

```
                              ┌──────────────┐              ┌──────────────┐
                              │ Pre-Approved │              │  Emergency   │
                              │    Change    │              │    Change    │
                              └──────▲───────┘              └──────▲───────┘
                                     │                             │
                                    Yes                           Yes

                                                          ┌─────────────┐
                                                          │  Is the     │
                       ◇                 ◇                │  change     │              ┌──────────┐
   ╭────────╮      ╱ Does the ╲      ╱ Has the   ╲        │ needed to   │     No    │  Normal  │
   │ Start  │─────▶  action    ──Yes──  process for ──No──  restore a    ──────────▶│  Change  │
   ╰────────╯      ╲ meet the ╱      ╲ this change ╱       │ critical    │           └──────────┘
                   ╲definition╱       ╲documented ╱        │ service and/│
                    ╲of a     ╱         ╲and      ╱        │ or outside  │
                     ╲change?╱          ╲pre-    ╱         │ of Change CI│
                        │                approved?         │ Maintenance │
                        No                                 │   window?   │
                        │
                ╭──────────────╮
                │ No change    │
                │ record is    │
                │ required     │
                ╰──────────────╯
```


8
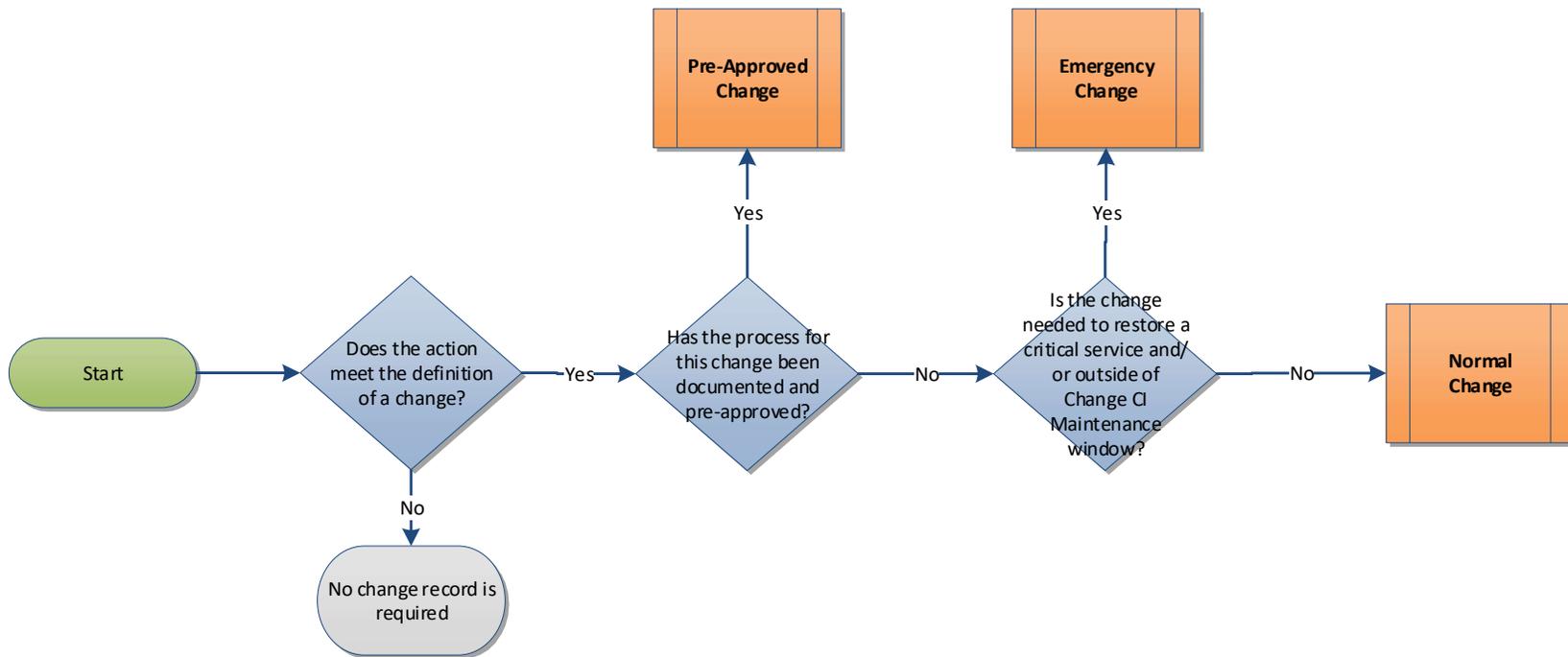
NORMAL CHANGE

OVERVIEW

A normal change is any managed change that:

- has not been pre-approved
- is not required to return a service or CI to normal operation, or is not outside of Change CI maintenance window

All normal changes must be:

- recorded in the change management system prior to implementation
- fully tested
- approved by Change CI Owner
- scheduled within defined change maintenance window
- communicated appropriately
- reviewed after implementation
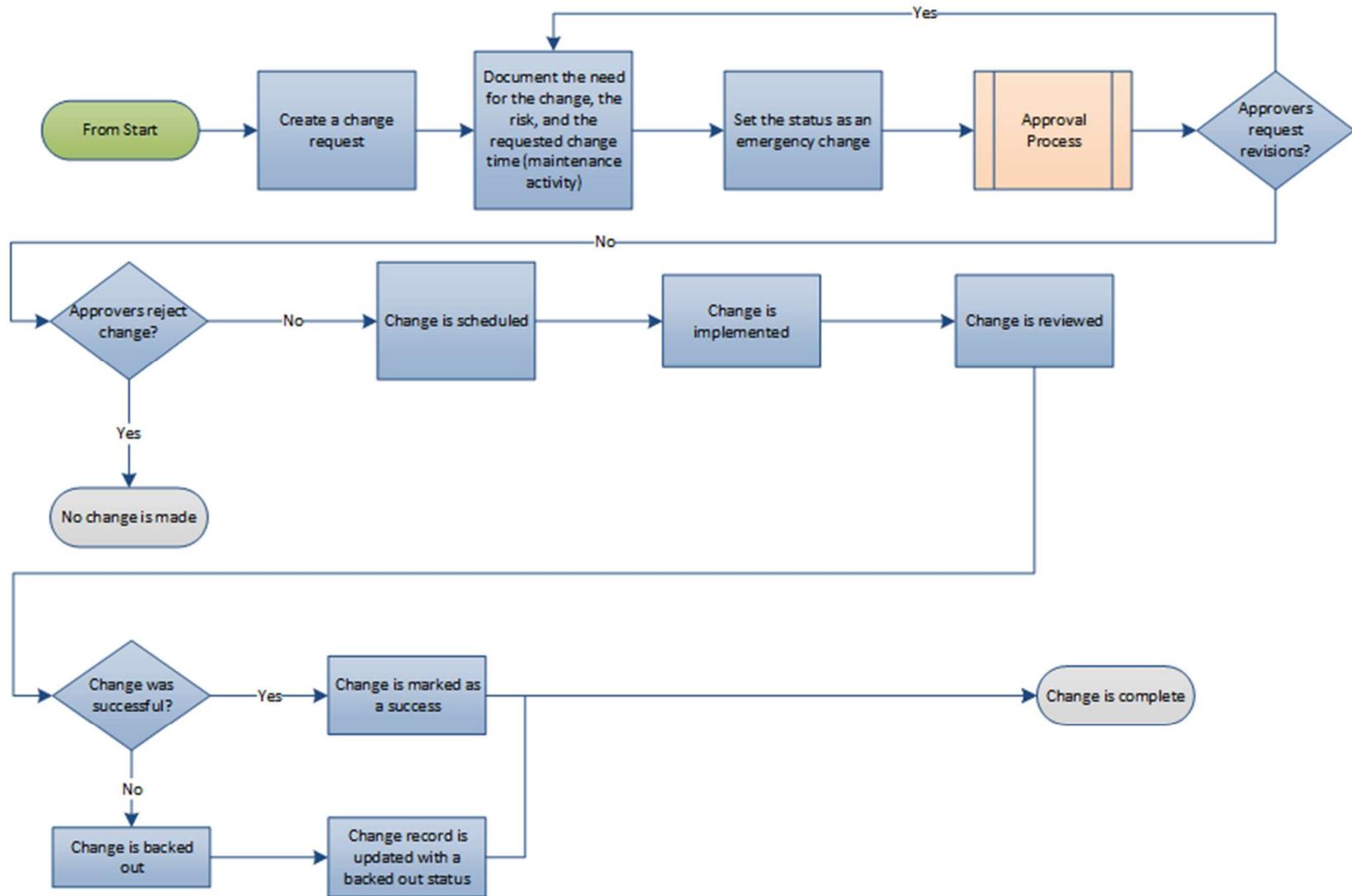
EMERGENCY CHANGE

OVERVIEW

An emergency change is any managed change that:

- is required to restore normal operation to a service or CI or is outside of Change CI maintenance window

All emergency changes must be:

- recorded in the change management system*
- approved by Change Advisory Board (CAB)in additional to the normal approval
- communicated appropriately
- reviewed after implementation
- linked to the incident regarding the outage in the change management system if applicable

*Due to the time-sensitive nature of emergency changes, the following actions are acceptable:

- initial approvals can take place outside of the change management system
- the change record can be created AFTER implementation

Emergency changes are the <u>only</u> classification for which the above actions are acceptable.

```
                                        Document the need
                                        for the change, the
  [From Start] → [Create a change  →    risk, and the      →  [Set the status as an → [Approval  →  <Approvers
              request]                  requested change        emergency change]      Process>      request
                                        time (maintenance                                            revisions?>
                                        activity)]                                                         │
                                                                                          ───Yes──────────┘

  <Approvers reject → No → [Change is scheduled] → [Change is → [Change is reviewed]
   change?>                                          implemented]
        │ Yes
   (No change is made)

  <Change was → Yes → [Change is marked as → ...... → (Change is complete)
   successful?>         a success]
        │ No
   [Change is backed → [Change record is
    out]                updated with a
                        backed out status]
```

PRE-APPROVED CHANGE

OVERVIEW

A pre-approved change is any managed change that has been pre-approved in advance and its change process has been documented. Pre-approved changes are generally very low risk and have been tested thoroughly. Pre-approved changes may be used to increase efficiency for recurring processes that do not require approvals each time they are made. Additionally, the pre-approved change workflow provides a simple and flexible framework to ensure that the unique needs of any given change can be met, while still meeting the overall goals of the change management process.

A pre-approved change process should be documented and each of the following aspects should be considered and documented:

- requirements (i.e., criteria that must be true for the change to be processed as a pre-approved change)
- how the change should be recorded
- when the change can be scheduled
- how the change should be communicated
- how the change should be implemented
- how the change should be reviewed

Pre-approved changes can be established by the same approver(s) that are identified on Change CIs. Please refer to the Approvals section for more information on how approvers are identified.

It is strongly recommended that changes be logged in a central location such as TeamDynamix. This will facilitate better communication and troubleshooting in the event that the change is disruptive. These changes can be recorded using an automated process so that they don't need to be manually entered.

FLOWCHART
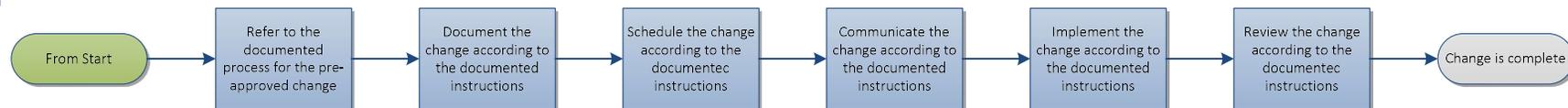
Name	Pre-approved Administrative Apps
Requirements	Used to track changes to Banner or one-shot with low/medium impact
Documentation	Change is documented in TeamDynamix and tied to a ticket or project
Schedule	As needed but usually after business hours
Communication	No communication is required
Review	The implementer will test the change and will roll back if needed

CUSTOM SOFTWARE CHANGE CONTROL- ON HOLD AFTER MIGRATION TO TEAMDYNAMIX 12/8/2025

Modification to custom software source code and implementation details, such as critical configuration and environmental settings, requires adherence to the standard processes of custom software change control managed in Citadel, a homegrown hosting platform. These change control processes are an extension of the C&IT Change Management Process. Adherence with the custom software change control processes satisfies the requirements of this document.

APPROVALS

OVERVIEW –

Before any change can be made, the approvers for the affected configuration item (CI) need to be defined. If the CI is only supported by one C&IT team, and the CI is not a dependency for any other teams, then the director of the responsible CI is responsible for identifying the approvers. If the CI is supported by more than one C&IT team, or if it's a dependency for a CI that another team supports, then the Change Advisory Board (CAB) is responsible for identifying the approvers. The association of CIs to approvers should be documented and available to those recording a change.
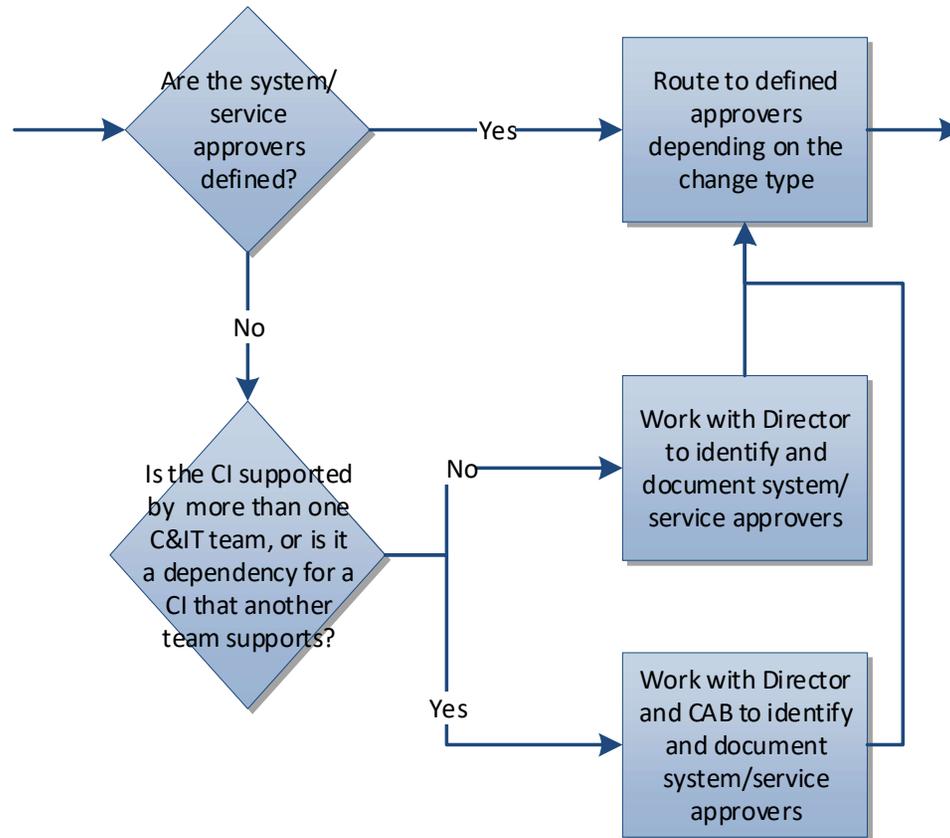
It is recommended that the list of CI approvers include individuals who:
- provide support for the configuration item (e.g., directors and/or team leads)
- support mission-critical systems or processes that are dependent on the affected CI (e.g., directors and/or team leads from other teams)
- may need to monitor and review changes to help avoid scheduling conflicts (e.g., Operations)
- need to be involved in decisions that could be highly disruptive to the university community (e.g., senior directors for emergency changes)

If desired, approvers can be defined differently for normal and escalation scenarios (out-of-window/emergency). Based on the needs of the CI, the approval system should support scenarios where only one approver in a list needs to approve or scenarios when all approvers need to approve.

The approver is ultimately accountable for the outcome of the change; it is the approver's responsibility to carefully asses the change and weigh the benefit to the risk of the change before approving. If the Approver for a change CI is not available (Vacation, out sick), the ITSM team can be contacted during business hours to approve the change. In order for the ITSM team to approve, they will need confirmation from the Approver's manager, SLT member or the CIO, if needed.

```
                    ┌─────────────┐
                    │ Are the     │
                    │ system/     │         ┌──────────────┐
                    │ service     │──Yes──→ │ Route to     │
          ────────→ │ approvers   │         │ defined      │────→
                    │ defined?    │         │ approvers    │
                    └─────────────┘         │ depending on │
                          │                 │ the change   │
                          No                │ type         │
                          │                 └──────────────┘
                          ↓                        ↑
                    ┌─────────────┐                │
                    │ Is the CI   │         ┌──────────────┐
                    │ supported   │         │ Work with    │
                    │ by more     │──No──→  │ Director to  │
                    │ than one    │         │ identify and │
                    │ C&IT team,  │         │ document     │
                    │ or is it a  │         │ system/      │
                    │ dependency  │         │ service      │
                    │ for a CI    │         │ approvers    │
                    │ that another│         └──────────────┘
                    │ team        │
                    │ supports?   │         ┌──────────────┐
                    └─────────────┘         │ Work with    │
                          │                 │ Director and │
                          Yes──────────────→│ CAB to       │
                                            │ identify and │
                                            │ document     │
                                            │ system/      │
                                            │ service      │
                                            │ approvers    │
                                            └──────────────┘
```

PROCESS MEMBERS AND RESPONSIBILITIES

Role	Description
Change Owner	The change owner is the individual responsible for coordinating and documenting the change. This does not necessarily need to be the person that is implementing the change, although it can be.
Change Approvers	The change approvers are responsible for approving normal and emergency changes before they are implemented. Change approvers can be unique for any given CI.
Change Advisory Board (CAB)	The CAB is comprised of members of C&IT's Senior Leadership team and IT Service Management. The CAB is responsible for identifying approvers in cases where a CI is supported by multiple teams, or when multiple teams are dependent on a CI. The CAB is also responsible for review and approval of all new Change Cis and emergency changes.

Change Process Owner	The process owner is responsible for:
	
	• advocacy/sponsorship of the process
	• ensuring value
	• lead the team in delivery of:
	    – overall process design
	    – defined measures (CSFs and KPIs)

Change Process Managers	The process managers are responsible for: • planning and coordination • checking input/outputs (auditing) • guiding practitioners (training, docs) • monitoring and reporting • providing guidance to the process owner when appropriate

CRITICAL SUCCESS FACTORS

- The change management process must be consistently used to track all changes within its scope
- All DSOE staff members responsible for implementing changes should be trained in the process and they should have a clear and concise understanding of the expectations of a change owner
- Configuration items should be defined in such a way that every property that could slow down the process (e.g., approvers, limited change window, etc..) should add clear value to the overall goals of the process

KEY PERFORMANCE INDICATORS

- Number of change records vs. same time period in previous year (target = higher)
- Percentage of successful changes (target = 90% or better)
- Number of emergency changes (target = less than 10% of all change records)
- Average amount of time for approval step on submitted changes (target = within one working day)
- Percentage of new C&IT staff trained in the change management process within first 2 weeks (target = 100%)