IT Change Management

A Practical Approach for Higher Education

EDUCAUSE WORKING GROUP PAPER

AUGUST 2018

EDUCAUSE

Table of Contents

This paper outlines steps to take to implement effective IT service change management. It provides guidance on defining your change, setting up your change management process (including roles and responsibilities, change management activities, RFC components, and risk and impact questions), and improving your process.

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.

There is no right process—when implementing change management, consider the organization, culture, roles and responsibilities, and what changes need to have change control. Ultimately, each organization needs to determine what change management practices work best for it.

Basic principles for change include the following:

- The change process should be as simple as possible while still meeting the objectives of the organization.
- The level of authority required to authorize a change should be commensurate with the level of risk the change poses to the organization.

- Organizations should decide what components are part of ITSM change control. Changes to components that affect the ability of the organization to deliver a service according to agreed service targets should have some form of change control.
- All parts of the service provider organization should use the same ITSM change process for components identified as being under change control.
- Changes to controlled components should be recorded in a central tool and made available to the whole organization.

This paper is for senior IT leaders, ITSM team directors, change managers, change advisory board members, and IT staff involved in change management. It is for use at institutions that are just starting out with implementing IT change management, as well as those that already have change management in place and would like to improve or enhance current processes. It outlines steps to take to implement effective IT service change management, including how to define change, setting up your change management process (roles and responsibilities, change activities, request for change components, and risk and impact questions) and improving your process.

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. Organizations choose what they want to control and the level of that control based on organizational needs. Things that might be controlled include hardware (servers, routers, switches, etc.) and software (purchased or developed in house), as well as less obvious items such as documentation, policies, contracts, processes, and management tools. The key to deciding what to control is to consider the benefit obtained versus the effort (cost) of controlling changes to the item.

When managing changes, it is helpful to classify the change. Three types of changes are commonly found in higher education: standard, normal, and emergency.[1]

- **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. Some organizations refer to these as *routine changes*. 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[2]), 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. Some organizations choose to classify normal changes based on risk, impact, or urgency. Typical classifications include major and minor:
  - **Major:** Poses significant risk or impacts the whole organization.
  - **Minor:** Presents some risk or impact to a smaller, well-defined part of the organization.
- **Emergency Change**: A change that is required to restore the normal operation of a service. Depending on local change authority (the change manager and CAB) requirements, the RFC for an emergency change might be submitted after the change has been implemented.

Setting Up Your Change Management Process

When designing a new change management process, it is important to remember that change management implementations can vary greatly from one institution

to another. The important point is to have a formal change management process. When first getting started with change management, pay attention to these points:

- Identify what your organization cares about and include that information in the change process.
- Get buy-in from all stakeholders, including IT staff/management and senior leadership, and include those stakeholders when designing your change management process.
- Find a "right size" model for your organization, community, and culture.
- Understand your resource limitations and develop a process that leverages/acknowledges those limitations.
- Identify what is in scope of your change management process (e.g., all operational changes, distributed changes, organizational changes, projects).

At a high level, change management starts with an idea that is then reviewed, authorized, and implemented. The change management process has touch points with other service management processes.

The change management process governs all change activities of the IT organization, and all changes are reviewed and authorized by the organization's change authority before any build and test activities are undertaken (see Change Management Activities). Many organizations focus formal change management on operational deployment—informal authorization is often given by leadership to build and test prior to when the formal change management process is invoked.

Working outside a change management process has risks. Organizations may lose transparency and be caught off guard when changes are proposed right before implementation. Changes might be delayed, causing frustration to the implementation/release team. There is no time to adequately prepare the IT organization, especially if the change is complex or has a high impact on the institution.

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. An organization's size, how it is structured, external partners, and other factors will influence how roles are assigned. The importance of role assignment is to achieve

consistency of accountability and execution. Following are common change management roles used in higher education.

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. These communications may be done by the requester, a dedicated communications officer, or other entity.
- Works with the change implementer to coordinate the change.

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. A change reviewer may not be required for every change. 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. Generally, the change approver:

- Is assigned based on the change being requested.
- 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.
- Closes completed changes.
- Coordinates postchange 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.

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. (See "Appendix A: The CAB" for more details.) Generally, members of the CAB ensure the following:

- 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 postimplementation 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.

Change Management Activities

Although implementation of changes will vary depending on the organization, the basic flow of the change management activities will remain much the same. Depending on the number of changes and the size of the institution, the number of people involved and the documentation required will vary. The activities listed in table 1 can help organizations starting to formalize their change management process.

Table 1. Change management activities

Activity	Description (Procedures)
1.1 Create Request for Change (RFC)	The change requester (or designee) follows the change management work instructions to create the RFC, including a risk and impact analysis (see table 2 for RFC components). The change implementer is assigned at this point in the process.
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 plan/build/test/deploy or implementation team as appropriate. If the RFC is rejected, it is returned to the requester with an explanation.
1.6 Communicate Change Details	The change requester and/or change implementer communicates the change details to the appropriate stakeholders. The mechanisms and the process surrounding change communication are determined as a part of the change management system and followed based on the type of change to be communicated.
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.

It can be useful to see these activities in a flowchart. Figure 1 shows a typical change process for a normal change. This figure not only shows the activity steps but also identifies the primary role for each step.

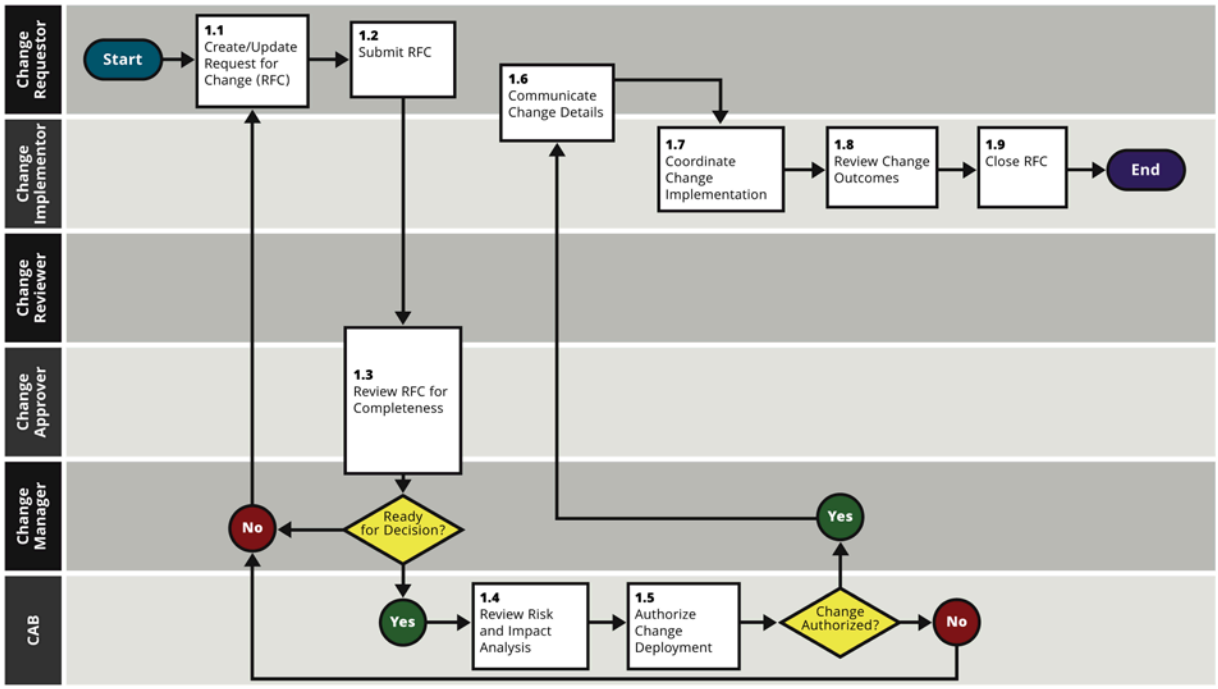

Figure 1. High-level change management process

Request for Change Document

The request for change is a formal document that outlines the change and expectations for making the change. An RFC should capture the information an organization believes is necessary to understand the change, why it is necessary, any risks associated with making the change, and how those risks might be mitigated. The makeup of this document depends on the organization's needs. The most common fields for a basic change request are identified in table 2.

Table 2. RFC components

Field	Description
Reference Number	A unique identifier that can be used to distinguish the RFC.
Submission Date	The date the RFC is submitted. If an automated system is being used to track change requests, this may be a system-generated field.
Change Requester	The name of the person requesting the change.
Change Implementer	A description of who is responsible for implementing the change.

Cont'd

Service or System Being Changed	A simple description of the service(s) or system(s) being changed.
Change Description	A description of the change. It should provide both an overview of the change and its scope and enough detail to understand what the change will accomplish and how it will be implemented.
Business Justification	A simple description of why the change is needed.
Date and Time of Change	The proposed implementation period for the change. It should include a start date and time and the expected duration (or an end date and time).
Risk and Impact Analysis	An assessment of the risks and impact of the change. This should include the scope of the change's impact (e.g., how many people are affected) and state the expected availability of the service or system during the change (e.g., whether there will be an outage).
Test/Validation Plans	A brief description of how the implemented change will be tested and validated to know if it was successful.
Remediation/Back-Out Plan	Details of what steps will be taken if the change implementation fails. The plan may take the form of a back-out plan for changes that can be reversed or may involve invoking the organization's continuity plan for changes that cannot be reversed. No request should be accepted or approved without a remediation plan. The plan details don't need to be included in the RFC, but there should be an acknowledgment that there is a documented plan, where to find it, and who would implement the plan if needed.
Communication Plan	Details of what is needed based on the nature and impact of the change to the organization. The plan should include known and possible impacts from change implementation, changes to how a user interacts with the service, and what process should be used to report issues after the change is completed. The plan details should include communication channels needed to inform all stakeholders and users affected by the change.

Risk and Impact

In the change management process workflow, the approval authority reviews the risk and impact analysis submitted as part of the RFC. A risk is defined as a possible event that could cause harm or loss or could affect the ability to achieve stated objectives. It can be considered as anything that might negatively affect the successful implementation of the submitted RFC. Impact is a measure of the effect a change has on people and business processes.

To facilitate a risk and impact analysis, the change authority needs information about every submitted change request. This information typically comes in the form of questionnaire answers that change requesters provide when submitting a change request. Recommended risk and impact questions are presented below as guidance for institutions establishing or revising their own change request submission process (see table 3). Typically, institutions assign a value to each answer. These values will assist in calculating the risk and impact of the change.

Table 3. Risk and impact

Risk and Impact Analysis Questionnaire
1. What is the designed scope of impact for this change? □ Enterprise-wide/all campus □ Division-wide/multiple large departments □ Location specific (e.g., a single building or small area; a single department) □ Small work team/small department 2. Is this a complex or high-risk activity? (Y or N) 3. Can this change potentially affect the availability, integrity, and/or security of other IT systems? (Y or N) 4. Has this change been tested? (Y or N) 5. Are any other units involved in making this change? (Y or N) 6. Are there any related changes involving different activities? (Y or N) 7. In what state will the system/service be during implementation? □ System/service outage □ Limited/reduced functionality □ Read only □ Normal functionality or handled by redundancy/HA (high availability) 8. When will this change occur? □ During a scheduled maintenance window? □ Nonpeak hours on nonpeak dates □ Business hours on nonpeak dates □ Anytime on peak days 9. What is the back-out effort? □ Difficult, impossible, or undesirable □ Possible, though not easily executed; would extend beyond the maintenance window □ In place and easily executed within the maintenance window □ Minimal

Improving Your Change Management Process

Implementing an IT change process is the first half of the battle. The other half is maintaining and improving the process. Oftentimes, compromises are made in rolling out the process. During initial operations, rough spots will be discovered. Over time, the needs of the organization will change, causing the process to be adjusted. Addressing these issues and other dynamics is the goal of continual service improvement.[3]

Any changes to the change management process need to be data driven. These changes should be made based on service goals that have been established. Change management metrics can be used to identify measurable improvements, driven by key performance indicators that support organizational goals. Some common metrics include the following:

- Failed changes
- Incidents caused by change
- Emergency changes
- Unauthorized changes
- Change requests rejected
- Change requests per service item

In addition, identifying pain points—parts of the change management process that cause frustration or don't seem to be working as well as they should—can also provide opportunities for process improvement, such as if there are complaints that the change approval process is taking too long or that necessary information isn't being gathered (or, alternatively, that unnecessary information is being asked for). It may be that training is necessary to help make sure that the RFC is being correctly filled out. Communication may need to be improved to help clarify the purpose and benefits of the process or to alert stakeholders of changes. Or it may be that the scope of change management wasn't clearly defined or did not account for all needs and therefore requires review and adjustment. As possible improvements are identified, it is important to keep track of and prioritize the opportunities (e.g., based on effort required to implement or value gained).

Perfection is never found in any process. To ensure that people continue to use the change management process and get value from it, teams must routinely check in to determine how to adjust the process as technologies and services change.

Conclusion

In its simplest form, a change is a response to stimulus. Change management provides tools to take a considered approach in responding rather than a reactive one. It does this by using standardized methods and procedures for handling changes. How an organization implements change management depends on the needs of the organization. A formal documented change management process has these benefits:

- Improved communication between the IT organization and the institution
- Smoother implementation of changes
- Improved teamwork throughout the organization
- Improved organizational awareness about IT changes and work
- Better appreciation and understanding of risk and impact related to changes
- More-reliable IT services

Who would not implement change management when you can have all these benefits?

Additional Resources

ITSM Frameworks

- ITIL IT Service Management Framework: ITIL is "the most widely accepted approach to IT service management in the world." See also the ITIL glossary.
- Lean Transformation Framework: Lean thinking "changes the focus of management…to optimizing the flow of products and services through entire value streams that flow horizontally across technologies, assets, and departments to customers.
- DevOps: DevOps is "a software engineering culture and practice that aims at unifying software development (Dev) and software operation (Ops)."

EDUCAUSE Materials and Communities

- EDUCAUSE Library, IT Service Management: The EDUCAUSE library includes a number of resources related to ITSM.
- EDUCAUSE Constituent Groups: These open, member-driven communities of practice offer a place to provide feedback on this paper, suggest topics for

new work, solicit advice from peers, learn about work others are doing, and more.

- IT Service Management (ITSM) Constituent Group: Topics include discussions of ITIL and ITSM processes implementations, usage of tools, training, and ways to promote a service management culture in higher education IT.
- DevOps Constituent Group: A forum for discussion and learning about the DevOps model of team IT management and service delivery.
- Business Relationship Management Constituent Group: Supports all IT professionals who act as the strategic interface between IT and IT business stakeholders for the purpose of solution discovery, relationship management, and participation in business IT strategy development.

Authors

Special thanks go to the following IT Change Management Working Group authors of this report:

Randall Alberts (Co-chair)
Assistant Director
Ringling College of Art and Design

Craig Bennion
ITSM Process Manager
University of Utah

Eric Dannenberg
Change & Configuration Manager
Boston University

Christina Foster
Services Transition & IT Operations Lead
The University of Oklahoma

Barbara Gosch
Change/Release Management Specialist
Minnesota State University System

Cris Harshman
Director Technology Services
Asheville-Buncombe Technical Community College

Mike Lenhart
ITS Consultant
The Pennsylvania State University

Thomas Mattauch (Co-chair)
ITSM Program Manager
Virginia Commonwealth University

Katie Rose
Senior Director User Services
University of Notre Dame

Elizabeth Rugg
Assistant Vice Chancellor, Client Engagement
University of North Carolina, Charlotte

Barbara Trainor
IT Manager, Business Client Services
Arizona State University

In addition, the working group would like to thank the EDUCAUSE ITSM Constituent Group Steering Committee for their review of this paper.

Notes

1. Your organization might identify additional change types as needed. Some common additional ones include:
   - **Test Change:** Test changes are implemented on nonproduction systems, have zero risk, and bypass the change advisory board (CAB) approval process.
   - **Out-of-Cycle Change:** These are normal changes that cannot wait for the next CAB for approval.
   - **Informational Change:** Changes that need to be added to the change schedule for communication purposes are called informational changes. Informational changes may be changes that are executed by a vendor but still need to be documented and communicated to the end user in the change system.
2. Change windows (also called *maintenance windows*) are set times when specific types of change or maintenance work may be performed. Some organizations choose not to have change windows but schedule the time as needed based on the work to be accomplished. Others are very specific—for example, changes to the financial application are pushed every Tuesday morning between 4:00 and 6:00 a.m. In some high-availability environments, changes can be implemented without any service interruption and so changes are pushed as needed, when needed. Alternatively, some organizations choose to have change moratoriums or freezes when no changes are allowed (e.g., at critical times of the year, such as during registration, beginning of the school year, sporting events, etc.). Using change/maintenance windows should be based on the value it provides to the organization.

3 For more information, see Doug Tedder, "Continual Service Improvement: The Six Steps to Success," *The Axelos Blog*, Axelos, June 16, 2015.

Appendix A: The CAB

The Change Advisory Board (CAB) is a group that comprises IT and business representatives—including managers and technical experts—charged with reviewing and approving changes. Chaired by the change manager, the CAB is charged with vetting all changes introduced into the IT environment. The CAB typically meets according to a regular schedule to review and authorize new change requests and perform postimplementation review of emergency and failed changes. Responsibilities also include the approval of standard changes.

Checklist: Setting up a CAB

- ✓ Define the purpose of the CAB.
- ✓ Identify a change manager to lead CAB meetings.
- ✓ Define who should participate in the CAB.
- ✓ Define how formal or informal the CAB meetings will be.
- ✓ Develop policies, procedures, and plans, including communication, etc.
- ✓ Decide what the approval process will look like.
- ✓ Define meeting frequency.
- ✓ Develop standard meeting and communication processes.
- ✓ Develop change calendar to help assess impact.

Purpose of CAB

The CAB's purpose is to evaluate changes and provide direction and support to the change manager. Some examples are:

- Help identify risks
- Ensure changes are well communicated and coordinated
- Ensure that there are no conflicts in the published change schedule
- Ensure that all changes are reviewed in a timely manner

Who Should Participate in the CAB

Each institution must define who should participate in the CAB. Change advisory boards may range in size and makeup. CABs typically include the change manager, individuals who can assess the technical and business impact of the change on other systems, and stakeholders. Defining who can assess the impact of the change varies; managers, directors, and technical experts are typically members of the CAB.

CAB Meetings

Each institution will need to decide a frequency and model for meetings and select a tool to keep track of all changes. CABs typically meet weekly, biweekly, or monthly. The ECAB meets as needed in response to an emergency change.

CABs can meet in any of several venues:

- **In-person:** All CAB participants convene in a physical location.
- **Virtual:** All CAB participants join an audio-only or audio/video call using a phone or computer.
- **Hybrid:** A hybrid model makes use of both in-person and virtual meetings. For example, the CAB may identify an in-person location and provide a virtual session for remote participants to join.

Attendance at the CAB is important and should be taken to identify who was involved in the decision-making process.

Typical Agenda

- Review all changes requiring approval
- Authorize standard changes
- Assess risks/unintended consequences and recommend risk mitigation
- Review conflicts and schedules
- Review failed changes

Appendix B: RACI Chart for Change Management Activities

The RACI chart below identifies common activities and who is responsible (R), accountable (A), consulted (C), and informed (I).

- **Responsible:** Those who do the work to achieve the task.
- **Accountable** (also approver or final approving authority): The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible. Very often the role that is accountable for a task or deliverable may also be responsible for completing it.
- **Consulted:** Those whose opinions are sought, typically subject-matter experts.
- **Informed:** Those who are kept up-to-date on progress, often only on completion of the task or deliverable, and with whom there is just one-way communication.

RACI Chart (responsible, accountable, consulted, and informed)

Operations Activities	Change Requester	Change Implementer	Change Reviewer	Change Approver	Change Manager	Change Process Owner	CAB	Stakeholder
1.1 Create Request for Change (RFC)	A/R	C		C				C
1.2 Submit RFC	A/R	C	I	C	I		I	I
1.3 Review RFC for Completeness	C		R	R	A/R			
1.4 Review Risk and Impact Analysis	C/I	C			A/R		R	C
1.5 Authorize Change Deployment	I	I		I	A		R	I
1.6 Communicate Change Details	R	R			A		I	I

Cont'd

1.7 Coordinate Change Implementation	R	R	I		A		I	I/C
1.8 Review Change Outcomes	C	R	C		A/R		I	C
1.9 Close RFC	C	R	I	I	A		I	I
Process Activities	**Change Requester**	**Change Implementer**	**Change Reviewer**	**Change Approver**	**Change Manager**	**Change Process Owner**	**CAB**	**Stakeholder**
Produce Monthly Metrics and Reports					R	A	I	I
Design, Manage, Document, and Improve Change Process	C/I	C/I	C/I	C/I	R	A/R	C/I	C/I
Train Staff on the Change Process	I	I	I	I	R	A/R	I	I

About EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 99,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information please visit educause.edu.

Citation for This Work

Alberts, Randall, et al., *IT Change Management: A Practical Approach for Higher Education*. EDUCAUSE working group paper. Louisville, CO: EDUCAUSE, August 2018.