

The University of Chicago



IT Services Change Management Framework

Version 3.0

june 1, 2017

Version	Date	Name	Reason For Changes
1.0	3/14/2011	Liss	Version 1
1.1	7/8/2011	Liss	Revised Change Type, Risk/Impact/Urgency analysis to reflect PwC audit requests Refined guidelines to reflect questions and precedents Separated Change Process Owner and Change Manager roles Updated system references to ServiceNow Misc. formatting and typo fixes
2.0	10/12/11	Liss	Revised Type and Request Level to better accommodate pre-analyzed changes and non-CAB-level changes Added Business Change Review to reflect PwC audit requests Minor clarifications/corrections/typo fixes
2.5	11/30/2012	Liss	Revised responsibilities for Service Owner and Service Manager Added QA Lite review Formalized CAB/EC review process Revised post-implementation reviews Minor clarifications/corrections/typo fixes
2.6	8/19/2013	Liss	Defined ticketing system of record (ServiceNow) and clarified the relationship between the system of record and subsidiary ticketing systems Removed data changes from scope of Change Management Established baseline for testing documentation
3.0	6/1/2017	Liss	Major re-organization and standardization as part of overall ITSM update Removed Major and Service Restoration as separate Types Formally introduced Major Change Proposal Streamlined risk/impact assessment Eliminated CAB/EC Aligned States and Close Codes to conform with ServiceNow out-of-box Clarified/streamlined approval processes Revised/clarified audit and review processes Revised/clarified communications

1.0	Overview.....	1
1.1	Background.....	1
2.0	Scope	2
2.1	In Scope.....	2
2.2	Out of Scope	2
3.0	Roles and Responsibilities.....	4
3.1	Roles and Responsibilities Matrix	4
3.2	Key Roles	10
3.2.1	Change Manager.....	10
3.2.2	Release Coordinator.....	10
3.2.3	Implementation Manager.....	11
3.2.4	Comparison of Roles	11
4.0	Processes.....	12
4.1	Change Request Standards	12
4.1.1	Summary of Types of Changes	12
4.1.2	Establishing Risk and Impact.....	16
4.1.3	Major Change Proposal.....	17
4.1.4	Required Approvals	18
4.2	Change Request Process Activities	21
4.2.1	Process Flow Charts.....	21
4.2.2	Planning, Building, and Pre-Implementation Testing.....	24
4.2.3	Initiating a Change Request	25
4.2.4	Approval and Scheduling	27
4.2.5	Implementation and Validation	28
4.2.6	Closing the Change Request.....	29
4.3	Change Management Administration.....	31
4.3.1	Change States	31
4.3.2	Review and Approval Bodies	32
4.3.3	Review of Completed Changes	34

4.3.4	Maintenance Windows and Blackouts.....	34
4.3.5	Defining and Documenting Standard Changes.....	35
4.4	Relationship to Other ITSM Processes.....	37
4.4.1	Service Request Management.....	37
4.4.2	Incident Management	37
4.4.3	Outage Management.....	37
4.4.4	Problem Management.....	37
4.5	Metrics	38
5.0	Communications	39
5.1	Ticketing and Systems of Record.....	39
5.2	Internal Communications.....	39
5.2.1	CAB Minutes and Reviews	39
5.2.2	Forward Schedule of Change	39
5.2.3	System Notifications.....	39
5.3	External Communications.....	40
5.3.1	Coordinating with Customers	40
5.3.2	Customer and Campus Notification	40

1.0 Overview

University of Chicago IT Services aims to continuously improve the operational processes used to support the services it provides. The overriding goal of these processes and related standards is to ensure best-possible operational efficiency, service, and uptime. This document addresses Change Management.

The objectives of IT Change Management are to:

- Increase the availability and reliability of IT Services computing infrastructure,
- Set accurate customer expectations regarding change impact,
- Minimize the negative impact of changes to customers, and
- Enable IT operations to move beyond reactive operation.

1.1 Background

Change Management delivers the processes and techniques required to allow IT Services to manage change associated with its Network, Hardware, Software, and Application Configuration Items (CI's).

IT Services staff support hundreds of servers (virtual and physical), network configurations, databases, and applications, resulting in a large and complex environment. A change to any one of these Configuration Items in production may introduce risk to functionality, availability, reliability, or performance. Managing changes to these Configuration Items mitigates risk and improves operating efficiencies.

Change management controls the introduction of change into an information system environment. It provides a detailed list of changes being scheduled to allow for balancing workload and resources. Without a clear understanding of current system configurations and control over how these configurations change, most other IT management functions fail. Its goals are to:

- Minimize and manage risk
- Reduce complexity
- Reduce exposure for human error
- Provide an audit trail of change to the environment to aid in incident logging, problem determination and incident and problem resolution
- Enable accurate performance analysis and reporting

Change management is a process that is part of the Service Support Set of Information Technology Infrastructure Library (ITIL). It is defined as an operational process; a function that must be performed. A change management process helps to identify and track changes, prevent conflicts between different changes, and isolate or eliminate subsequent problems.

2.0 Scope

IT Change Management is the enterprise-wide process of implementing approved changes efficiently, and with acceptable risk to existing and new IT services. This involves scheduling, documenting, approving, communicating, implementing, testing, and monitoring changes to all IT Services production environments.

The production environment is defined as the configuration of network, hardware, software, and applications in support of a service for internal or external customers.

The IT Services Change Management process applies to all changes in the production environment. Only changes that comply with the Change Management process will be accepted into production. A change is an action; the addition, modification, alteration or deletion of one or more IT Services Configuration Items in the production environment, or the addition, alteration, or removal of environmental equipment in the Data Center (e.g. HVAC, UPS) which carries an element of risk to production services.

2.1 In Scope

The scope of the current Change Management process includes:

- *Normal, Standard, and Emergency changes to production IT infrastructure and applications.*
- *Review and approval of documented implementation plans for Standard Changes.*

2.2 Out of Scope

Exceptions to the scope of Change Management includes:

- *Data Changes* – Changes to data, including large-scale cleanup projects, are not considered Changes. This does not mean they are exempt from tracking in general, but they should be tracked as projects or Service Requests rather than being submitted to the Change Management process. (Note: Configuration changes are never considered to be data changes. Also, if the data being changed will be fed into other systems, and the downstream applications may use the data for authorization or other purposes which affect how the application acts, then that is also not considered a data change.)
- *Non-Production Applications* – New applications which have not yet been deployed are not subject to Change Management until such time as they are moved into production. Development and test environments are also not subject to Change Management. (Note that infrastructure environments which exist to support multiple dev/test environments are actually production – for example, a storage device which hosts only dev/test systems is considered to be in production and subject to Change Management, even though this is not the case for any of the dependent systems. Also note that any system being hosted for a third party should always be considered production from a central IT standpoint, even if the client users are not using it for production purposes.)
- *Custom Workgroup Applications* – Applications custom-written for small workgroups (<10 people), where outages of this application will have no impact beyond the workgroup. Changes to these applications should still be recorded and tracked, but they are not subject to IT Services Change Management processes.
- *Exempted operational activities* – Service Owners and Service Managers may, when submitting Standard Changes for review by CAB, also submit a list of activities which are considered extremely common, low-risk, and low-impact, but also necessary for day-to-day maintenance of services. CAB may then elect to exempt these activities from Change Management. If these activities are later shown to cause outages or

incidents, then the Change Manager may revoke this exemption, either for specific services or in whole, and require the activity to go through Change Management from that point forward. See section 4.3.4 for more information. (Note that activities which take place during scheduled maintenance windows are not automatically exempted. An activity must be explicitly documented and reviewed by CAB to qualify for an exemption. See section 4.3.4 for more details.)

- *Automated Patching Cycles* – Automated patching is considered to be an exempted operational activity by default, as long as it meets the following criteria:
 - Systems being patched must only host non-critical services
 - Automated patches must be applied during scheduled maintenance windows according to a fixed and documented schedule (e.g. “second Wednesday of each month”)
 - Only the application of patches is exempted; changes to patch schedules or to the automation process itself are still subject to Change Management
 - Patches which are applied out-of-cycle or otherwise outside the automation process are subject to Change Management
 - The Change Manager may revoke this exemption for any service if automatically applied patches cause an outage or multiple incidents for that service

3.0 Roles and Responsibilities

3.1 Roles and Responsibilities Matrix

The following table lists the primary roles involved in the Change Management process and their associated responsibilities. Note that it is possible for one individual to be in multiple roles (e.g., if a change has an Implementation Manager, that person is often also the Change Owner). Also, while some roles can only have a single individual in them for any given change (Change Owner), others may have multiple individuals, possibly spanning several groups in ITS.

Table 1. Roles and Responsibilities

ROLES	RESPONSIBILITIES
Business Approver	- Defined as a single individual who is responsible for a business process which is being affected by an IT change to a Financially Significant Application - Responsible for reviewing and approving the change before it can be implemented (generally approving UAT results and the proposed change schedule) - May be an ITS Service Manager if the change is purely internal and does not affect user interaction with the system (e.g. updates to back-end administrative interfaces)
Business Owner	- Defined as a single individual with overall understanding of the business objectives and functional processes which are enabled or fulfilled by the Service. The Business Owner often has strategic and/or operational authority over the business processes in question. - Review and approve proposed changes which add, remove, or modify business functionality, or which would have substantial business impact (e.g. an extended disruption outside normal maintenance hours) - Work with Service Owner to ensure that Changes are communicated to the user community as appropriate - May delegate these duties for Standard changes or low-impact Normal changes but remains accountable for ensuring that they are done
Change Advisory Board (CAB) (see section 4.3.1.2 for more information)	- Members represent IT areas that design, implement, or are affected by Change Requests on a regular basis. - Assess, authorize, and schedule all Normal Change Requests - Review and approve documentation for Standard change plans and workflows - Responsible for preparing for and attending reviews and following up on issues involving their areas. - Possess key expertise necessary for ensuring the Change Requests affecting their areas are planned, tested, and implemented correctly

ROLES	RESPONSIBILITIES
Change Liaison	• Responsible for working with the Change Owner to coordinate activities or communications outside the Change Owner's workgroup • Usually a Technician when in another group in ITS • May also be in a key business area which needs to approve UAT, validate a change's success, and/or communicate information about the change to end users

ROLES	RESPONSIBILITIES
Change Manager (see section 3.2.1 for more information)	• Manage the day-to-day change process: ○ Assure there is a functional Change record. ○ Mediate conflicts related to the change (if required). ○ Approve changes based upon risk mitigation. ○ Review change plan and ensure its adherence to standards. ○ Ensure client communication is completed according to IT Services change standards. ○ Review completed changes to ensure processes/standards were followed. Identify follow-up actions; direct closure of change records. ○ Chair the CAB and Emergency Change Advisory Board (ECAB) ○ Identify additional approvers as appropriate for higher-risk and Emergency changes. ○ Identify potential time conflicts during which multiple changes may be planned. ○ Coordinate with Service Owners to develop group procedures and policy in accordance with Change Management Framework. ○ Aid in identifying and documenting Standard Changes. ○ Facilitate understanding of Change Management policy and procedures. ○ Manage the change management calendar ○ Enforce process and standards, and work to improve process. • Own the Change Management Process: ○ Accountable for the entire Change Management process. ○ Analyze the effectiveness of the change process. ○ Obtain and publish metrics that demonstrate effectiveness of change management processes with an emphasis on the reduction of high impact incident counts and duration. ○ Identify and lead implementation of necessary improvements. ○ Ensure procedures, tools, and documentation are updated. ○ Develop and maintain standard change and operational activity exemption review processes. ○ Lead integration of change management process with other processes. ○ Update IT Services management on the state of change management.

ROLES	RESPONSIBILITIES
Customer	• An internal IT Services associate or external associate who requires the production environment in order to perform their job. They may be one of many groups who can request a change.
Emergency Change Advisory Board (ECAB) (see section 4.3.1.3 for more information)	• Ad hoc group convened by Change Manager • Review and approve risky or impactful Emergency Changes when the need for these changes arises during an outage or between regular CAB meetings
Implementation Manager (see section 3.2.3 for more information)	• Approve change plan including back out plan ○ Identify and approve change tasks ○ Identify back out plan and criteria for deploying it ○ Identify change milestones • Lead change implementation ○ Identify the change implementation team ○ Make sure team members understand the change ○ Secure a war room or conference bridge if necessary • Lead communication during the change. (IT Services Communications should be involved in notification regarding campus-wide problems, per existing processes) ○ If necessary, write a standard statement for the Service Desk to communicate to clients if many calls are being received or are anticipated. This ensures a standard message to all customers ○ Direct communication to internal IT Services staff ○ Verify that interim and follow-up communication to all customers is completed ○ Write and/or edit information distributed to customers ○ Communicate with IT Services management at your discretion ○ Communicate with IT Services Liaisons, IT Services staff, and vendors as appropriate ○ Evoke Incident management or Outage management standards if necessary

ROLES	RESPONSIBILITIES
Change Owner	• Accountable for overseeing the implementation of a given change and validating its success or failure • Prepare & Maintain Change Plan • Responsible for ensuring that changes they perform are appropriately documented in a Change Request and have received appropriate approvals prior to implementing the change • Help with documentation and monitoring • Coordinate response to customer concerns regarding planned changes • Uphold IT Services change standards and process • Promote inter-group change coordination and cooperation • Coordinate change activity • Maintain technical support response documentation • Provide business impact analysis of a change • Provide business impact analysis of any incident resulting from this change • Communicate change and its impact to IT Services leadership • Implement approved changes. • Evoke Back-out plan if necessary
QA Lite (see section 4.3.1.1 for more information)	• Review changes to financially significant applications prior to CAB review, with explicit attention to: ○ Evaluating business impacts of proposed changes; ○ Ensuring changes are assigned proper risk and impact levels; and ○ Confirming that changes are properly tested before production deployments, including UAT signoff and business approval
Release Coordinator (see section 3.2.2 for more information)	• Make sure that the new or upgraded service is understandable to end users ○ Work with IT partners or key customers to understand user needs ○ Liaise with VIP support and faculty bodies to make sure the service is rolled out properly at a VIP level ○ Work with IT Communications and others to develop and execute a formal communications plan and ensure proper end user documentation • Work with Service Desk and SMEs to make sure they have the information, access, and tools they will need to support the service ○ Ensure appropriate support documentation, processes, and workflows • Guide the new service through the New Service Rollout process

ROLES	RESPONSIBILITIES
Service Manager	• Defined as a single individual who is responsible for day-to-day operational delivery of a defined Service in accordance with business requirements. • Review and approve normal operational changes to the service • Review and approve emergency changes to the service • Accountable for developing and maintaining plans and workflows for Standard Changes and submitting them to CAB for review • Ensure appropriate representation at any CAB or other change review discussions to provide technical detail and address concerns regarding a change to the service that is being reviewed • Work with Lead Technician to ensure that proposed changes have appropriate implementation, backout, and test plans • Work with Service Owner to ensure that appropriate communications will take place
Service Owner	• Defined as a single individual with overall understanding of both the high-level technology and business functions of the service. The Service Owner is accountable for the overall direction of the service, including its sustainability for meeting business objectives, ongoing development, and transformation. • Coordinate communications • Accountable for ensuring that all changes to the Service are appropriately documented in a Change Request and have received appropriate approvals prior to implementing the change • Work with Business Owner to review changes which would have substantial business impact (e.g. an extended disruption outside normal maintenance hours) • Ensure appropriate ongoing representation in CAB for awareness, review, and discussion of changes in all areas of the organization which may have an impact on the service • Assign a Release Coordinator and/or Implementation Manager as necessary
Technicians	• Identify necessary changes • Identify anomalies that may indicate the need for change • Identify and communicate technical risks to the Service Owner, Service Manager, and Change Manager • Work with Change Owners to implement approved changes as necessary

3.2 Key Roles

3.2.1 Change Manager

3.2.1.1 Role

The Change Manager owns the Change Management process as a whole, ensuring its utility and fit to the IT Services organization and coordinating with management and staff to ensure smooth planning, review, scheduling and execution of changes. The role ensures that all changes to IT services receive appropriate approvals and communications to the IT organization and to the campus as a whole.

3.2.1.2 Involvement

Change Manager is an ongoing role within the Change Management process. The Change Manager chairs the Change Advisory Board (CAB); convenes Emergency CAB meetings when necessary; and monitors changes and the change management process continually to ensure its smooth operation and smooth interface with other ITSM processes, especially Problem and Service Request.

3.2.2 Release Coordinator

3.2.2.1 Role

Release Coordinator is a management role invoked in longer or more complicated changes, especially those which involve the rollout of a major new service or a transition to an existing service which will have a significant ongoing operational impact on end users (e.g. an upgrade which requires re-training, or a transition which require users to take some action). This role ensures management involvement in communications, coordination, and business decisions encountered while planning the change and release deployment. Properly speaking, this role should be part of the Release Management process, but is being incorporated in Change Management pending development of an ITS Release Management program.

3.2.2.2 Involvement

Assign Release Coordinator to any change which will require significant coordination and communication with end users to ensure a smooth rollout. Often the Release Coordinator will also be the Project Manager for the project which is developing the new service or service transition, but it may also be a business analyst, communications expert, or other SME who is called in to help identify user-facing issues connected to the change and help develop and document solutions for those issues. The Release Coordinator is involved from the beginning of the change planning phase (if not sooner), and may remain involved with the service rollout beyond the change's implementation, aiding in post-implementation communications and incident resolution.

3.2.3 Implementation Manager

3.2.3.1 Role

Implementation Manager is a management role invoked in longer or more complicated changes, especially those which involve extended outages to essential or critical services. This role ensures management involvement in communications, coordination, and business decisions encountered during change implementation.

3.2.3.2 Involvement

Assign Implementation Manager immediately to any Major Change. Usually the Implementation Manager will also be the Change Owner, but the role may instead be assigned to a Project Manager or to the Service Manager associated with the change. It is the responsibility of the Service Owner to assign an Implementation Manager when necessary. If a change involves multiple services or critical infrastructure, the Service Owner or CAB may require that the Implementation Manager be on site during the implementation of the change.

3.2.4 Comparison of Roles

Table 2. Comparison of Release Coordinator and Implementation Manager Roles

RELEASE COORDINATOR	IMPLEMENTATION MANAGER
• Strategic focus on service rollout/transition • Develops user requirements which will ensure a smooth service rollout • Coordinates communications to users before and after the change • Works with Service Manager to ensure that necessary user documentation is created or updated • Monitors execution of the change • May continue communications involvement after execution of the change	• Tactical focus on change implementation • Develops change plan to meet user requirements for smooth rollout • Manages communication to users and ITS management during the change • Generally not concerned with user documentation • Manages and coordinates execution of the change • Duties usually end once change ticket is reviewed and closed

4.0 Processes

4.1 Change Request Standards

4.1.1 Summary of Types of Changes

In order to expedite the change review and approval process, change requests are divided into three different types; the type of change request determines what approvals are necessary and guides the planning and communication processes.

- **Standard Changes** are common, low-risk changes which follow a standard, repeatable implementation process. The CAB reviews and pre-approves the implementation process, thereby allowing the change to be performed as necessary without further CAB review as long as it can be done within the pre-approved process. **Maintenance Activities** are a special class of Standard changes which are regarded as so common and so low-risk that they do not require tracking.
- **Emergency Changes** are changes which must be implemented quickly to resolve an ongoing incident or prevent an incident from occurring (e.g. installing a critical security patch). They undergo an abbreviated review and approval process to reflect their urgency.
- **Normal Changes** are all changes which are neither Standard nor Emergency. In general, the CAB reviews (or has the option to waive review) all Normal changes. **Major Changes** are a special class of Normal changes which receive more scrutiny due the degree of disruption or risk they entail (see section 4.1.3 for more information).

The table below provides general guidelines and criteria for determining Change Type.

Table 3. Types of Changes

TYPE	DEFINITION	EXAMPLES	HOURS/DAYS	WORKFLOW
Normal	Requested change could potentially affect the functionality of an existing service and/or production applications	• Application upgrade • OS upgrade • Changes to existing cabling or hardware configuration where these changes could affect service • Potentially service-impacting DNS changes • Service-impacting VM configuration changes	• During standard change windows, OR • As approved by CAB and business owners	Normal changes must have their project plans approved by appropriate management. Change request must be submitted for CAB review at least 7 calendar days prior to date of change For Financially Significant Applications, QA Lite must review prior to CAB. Implementation Manager or Release Coordinator may be required.
Major	Requested change could potentially affect the functionality of several existing services and/or production applications; OR Requested change requires disruption of Critical or Major service outside regularly scheduled maintenance; OR Requested change could potentially have financial, legal, regulatory, or life/safety ramifications, or affect the image or reputation of the University	• LDAP upgrades • Platform network upgrades • Service-impacting DNS changes • Service-impacting VM configuration changes	• Maintenance Window required • Exceptions require approval	Major Change Proposal must be submitted at least 28 days prior to requested date of change. Remainder of workflow and approvals as per Normal changes.

TYPE	DEFINITION	EXAMPLES	HOURS/DAYS	WORKFLOW
Standard	Tested maintenance that will be applied in the same way to many similar systems Common changes that do not necessarily require management approval or scheduling and may be sufficiently low-risk/low-impact that they can be performed during business hours	• OS Server patches • Windows Service packs • Routine updates to feeds and reports	During maintenance windows or as defined in pre-approved Standard change plan	• Technicians must perform testing and review the tested maintenance before it can be applied to production systems. • Group management must approve planning and scheduling. • Business approval required for changes to Financially Significant Applications. • To be classified as a Standard change, a standard change plan must be pre-approved by the CAB.
Maintenance Activities	Simple, extremely low-risk, non-intrusive activities that are performed routinely during maintenance windows or as needed; does not involve configuration changes	• Clearing log files • Weekly system or service restarts • Automated, regularly scheduled patching to non-critical servers or systems	During maintenance windows or as pre-approved by CAB	• Must be defined, documented, and approved as a maintenance activity by CAB • Does not require a Change ticket

TYPE	DEFINITION	EXAMPLES	HOURS/DAYS	WORKFLOW
Emergency	An emergency change is a response to an unplanned problem or security risk, and must be made as soon as possible due to significant urgency (proactive); emergency changes are also performed to resolve ongoing incidents (reactive).	• Failure of one component in a redundant architecture results in lack of redundancy • Critical security patch related to a security exploit known to be active “in the wild” is released • Situation indicative of impending (but not immediate) failure • Replacing a failed switch to restore network service • Applying patch or configuration change to restore or stabilize a failing application	Where possible, emergency changes should be planned during regular maintenance windows. If it is not reasonable to wait for a change window, the time planned should allow as much time as possible to minimize the effect on customers.	Proactive Emergency changes must receive workgroup and Change Management approval before the change is implemented. Change Management may invoke an Emergency CAB as appropriate. Reactive Emergency changes must receive verbal approval from the appropriate manager or director before proceeding, and must be documented (and retroactively approved) in-system within 24 hours of the change activities. Reactive changes must also be associated with the Incident tickets they are responding to.

4.1.2 Establishing Risk and Impact

4.1.2.1 Risk

Risk is a combination of three factors: Change Complexity, Change Interdependency, and Implementation Experience.

- Change Complexity indicates the number of steps required to execute the change
 - Complicated – the change has many steps
 - Average – the change has a moderate number of steps
 - Simple – the change has one or very few number of steps
- Change Interdependency indicates the number of interdependencies required to execute the change activities.
 - Complicated – The Change is one of a group of Change activities that must be executed within the same Change Window and the activities in the group are not the same
 - Average – The Change is one of a group of Change activities that must be executed within the same Change Window and all of the activities in the group are the same.
 - Simple – The Change may be executed independently of other Change activities
- Implementation Experience indicates the collective ability of the organization to successfully execute this Change
 - No Experience – The organization has no experience with this type of Change
 - Limited Experience – The organization has only limited experience with this type of Change and/or the procedure is not fully documented (a SOP does not exist).
 - Proven Experience – The organization has repeatedly executed this type of Change successfully in the past and the process is fully documented (a SOP exists).

Once Complexity, Interdependency, and Experience have been determined, Risk is calculated as follows:

- If either the Change Complexity or Change Interdependency is complicated or we have no experience with this type of change then the Risk is said to be **High**.
 - Otherwise, if either the Change Complexity or Change Interdependency is average or we have limited experience with this type of change then the Risk is said to be **Medium**.
 - Otherwise the Risk is said to be **Low**.

Risk may be adjusted upwards or downwards if extenuating circumstances exist. Possible examples include:

- Complicated interdependencies between the service being changed and other services which could be adversely affected by the change (adjust upwards)
- A class of change we have successfully executed repeatedly in the past has recently caused incidents (adjust upwards)
- Multiple layers of redundancy exist and can be used to mitigate the likelihood of an Incident (adjust downwards)
- The technician performing the change is not personally experience with this particular kind of change (adjust upwards)

When assessing risk, it is better to err on the side of a higher risk than a lower one. If there is any doubt, the Change Manager or the Change Advisory Board should be asked for clarification.

4.1.2.2 Impact

Impact is a rating of how severely University business could be affected if this change causes a problem. This rating includes the likelihood of indirect impact as well a direct impact – if a change could potentially impact not only the service being changed, but other, “downstream” systems and services as well (e.g. via data feeds), then the potential impact on these downstream systems is taken into account. Note that there may be ways to mitigate a change’s impact; for example, a change done during a time of year when a system is seeing little use may have a lower Impact rating than a change done during that system’s busy season.

Table 3. Impact Level

IMPACT RATING	EXAMPLE
High	>1000 users affected Cascade effect on multiple systems/services Direct financial, legal, regulatory, or life/safety repercussions May affect image or reputation of the University Major business function disrupted campuswide at critical time
Moderate	100-1000 users affected Major business function disrupted campuswide at non-critical time Multiple non-critical workgroups/business functions disrupted
Low	<100 users affected No business disruption above the level of a single department/workgroup

Impact may be assessed upwards or downwards if extenuating circumstances exist. Possible examples include:

- Political sensitivities which warrant extra scrutiny and care around the change (adjust upwards)
- Change is being scheduled at a time when few or no users are using the system (e.g. well outside business hours or during interims) (adjust downwards)

When assessing impact, it is better to err on the side of a higher impact than a lower one. If there is any doubt, the Change Manager or the Change Advisory Board should be asked for clarification.

4.1.3 Major Change Proposal

A Major Change is considered to be any change which is High Risk-High Impact; High Risk-Medium Impact; or High Impact-Medium Risk. Typically these are significant, disruptive (or potentially disruptive) changes to high-profile business applications or critical infrastructure. Accordingly, they have a higher standard for planning and communication than changes with a lesser risk/impact profile, and will receive greater scrutiny from CAB. In many cases, a Major Change may even arise from a Project and be received by change management as a series of Change Requests, whose interdependencies must be understood and taken into account when reviewing them.

In order to streamline this process, when a Major Change is being planned, the Service Owner is accountable for submitting a Major Change Proposal to the Change Manager at least one month (28 calendar days) prior to the planned implementation date (or the first implementation date, if multiple Change Requests are involved). Often, the Service Owner will delegate the responsibility for the Proposal to the Service Manager, Release Coordinator, or Implementation Manager for the change.

The Major Change Proposal contains:

- A high-level description of the change and the expected results (a new or changed service)
- Resources and groups required for the change
- Pre-implementation test plans
- Impact of the change, including any expected service disruptions, potentially affected dependent services, changes to business process or user interaction with the service, and affected audiences (including impact on Medical Center and offsite locations)
- A high-level description of the change plan and implementation schedule, including validation planning
- Backout plan information
- Major risks and mitigation strategies (including risks involved with not performing the change in the target timeframe)
- Communications planning, including planned training, end-user documentation, and internal documentation
- Post-implementation support plans, especially if there is the possibility of emergency or stabilization changes to address defects that were not identified or addressed in pre-implementation testing

The Change Manager will review this documentation and provide feedback on constructing the final change plan and accompanying Change Request to ensure minimum back-and-forth when the request is reviewed by CAB. Depending on the exact scope of the change, the Change Manager may consult with other service owners, subject matter experts, and organizational leadership in this review to make sure that potential conflicts or business concerns have been adequately addressed.

4.1.4 Required Approvals

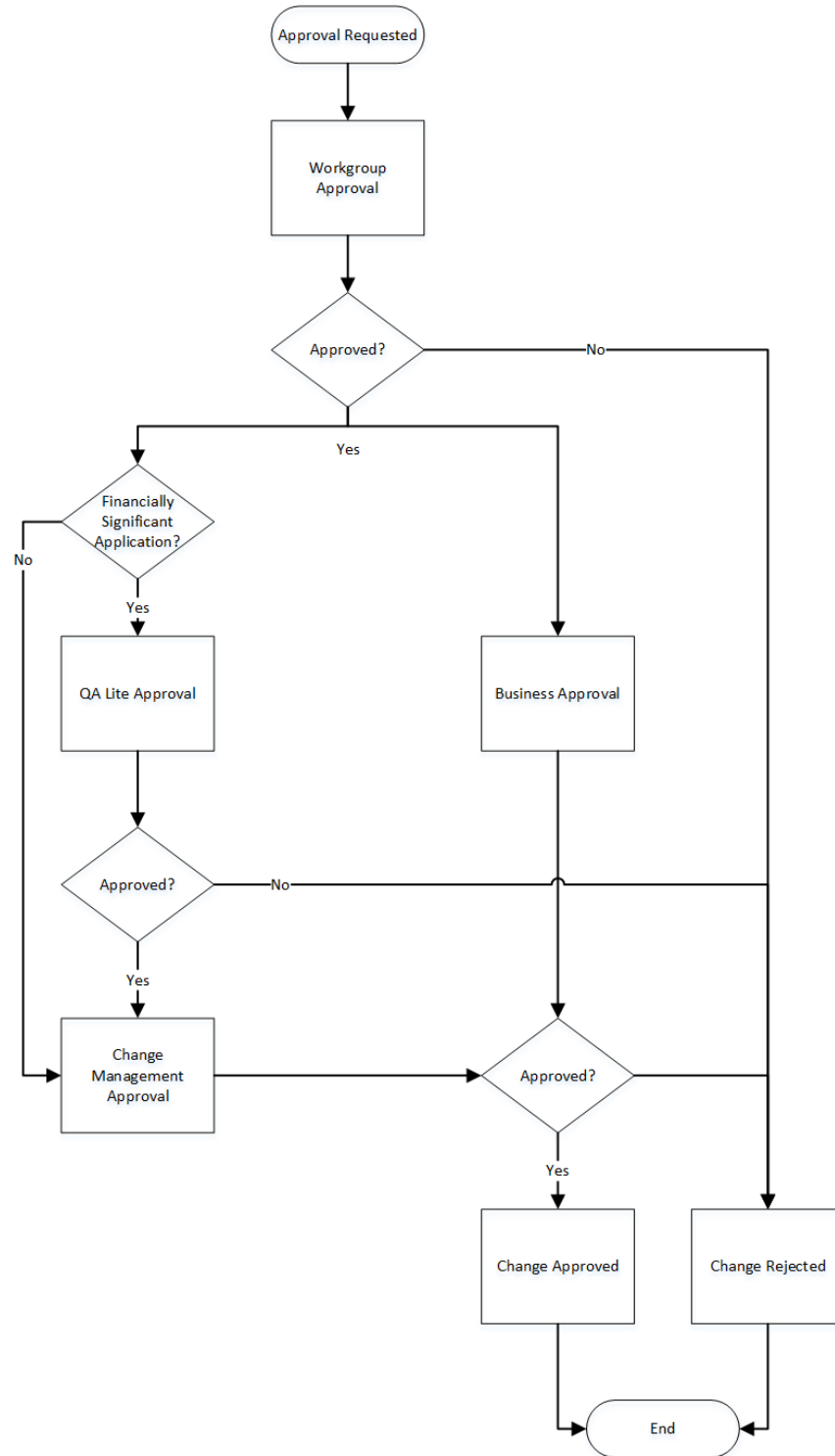
All changes must undergo approval, based on the Change Type and the service being changed. There are four layers of approval. The basic two are Workgroup Approval and Change Management (or CAB) Approval. In addition, changes to Financially Significant Applications must potentially receive QA Lite Approval and Business Approval.

- **Workgroup Approval** is the gateway before other, later layers of approval. Each workgroup must have at least one assigned individual who reviews and approves all changes assigned to the workgroup. By default, this group will always include the Manager for that workgroup, but may also include a Director, Service Owner, senior technician, project manager, or other trusted individuals. When defining Standard Changes, the Service Owner and Service Manager may ask CAB to waive Workgroup Approval for very common, basic changes, especially changes in response to Service Requests; if CAB agrees, then these changes may proceed without explicit Workgroup Approval for every instance of the change. Apart from these CAB-approved exceptions, all Standard, Normal, and Emergency changes must receive Workgroup Approval before passing on to later approvals. Reactive Emergency changes to address ongoing incidents will often be created after the fact, and therefore reviewed and approved at the Workgroup level after the fact.
- **Change Management Approval** applies to all Normal and Emergency changes. In general, this consists of a CAB review for Normal changes; however, the Change Manager may elect to waive CAB review for Low Risk/Low Impact Normal changes on a case by case basis in urgent situations. For proactive Emergency changes, the Change Manager has the discretionary authority to submit the change to CAB for an ad hoc review, or to convene an ad hoc Emergency CAB to review the ticket, depending on the timing and urgency of the request. (See section 4.3.1.3 for further information on the ECAB.) Reactive Emergency changes to address ongoing incidents will often be created after the fact, and therefore reviewed and approved by Change Management after the fact.

- **QA Lite Approval** takes place between Workgroup Approval and Change Management Approval, and reviews requested Normal changes to Financially Significant Applications for potential audit issues. See section 4.3.1.1 for further details.
- **Business Approval** is required for all Standard and Normal changes to Financially Significant Applications to confirm that the proposed change meets business requirements and passes User Acceptance Testing. Other services may also elect request Business Approval for some configuration items if it seems appropriate; this determination is made by the Service Owner. Business Approval is done after Workgroup Approval (and in parallel with QA Lite and Change Management approvals for Normal changes). If a formal Business Approver has not been assigned, then approval is requested ad hoc from the business according to processes governing the service in question, and appropriate documentation attached to the Change Request.

4.1.4.1 Approval Workflow

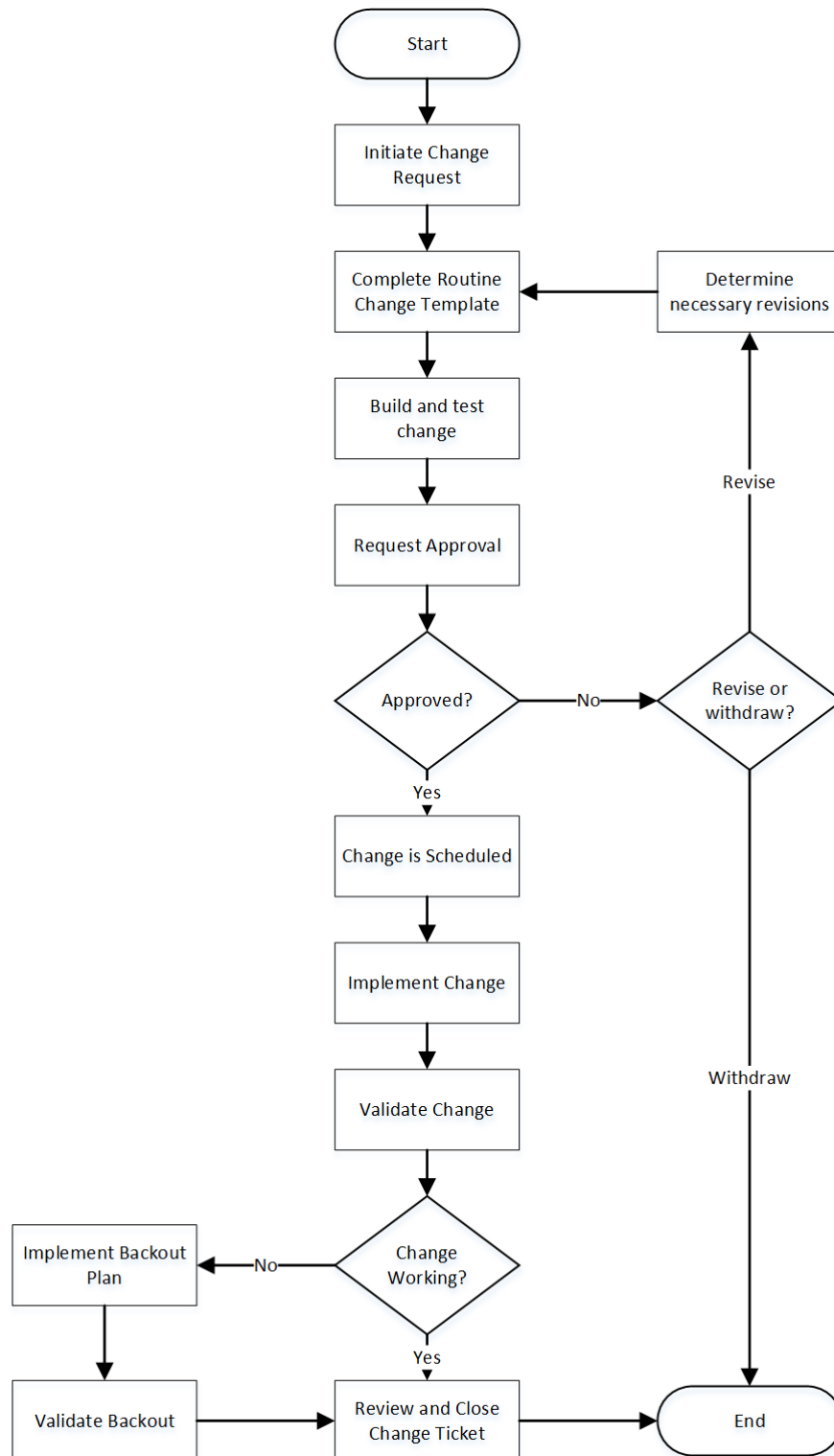
The diagram below illustrates the Approval process for Normal changes. Standard Changes automatically waive Workgroup, QA Lite and Change Management approvals; Emergency Changes automatically waive QA Lite and Business approvals.



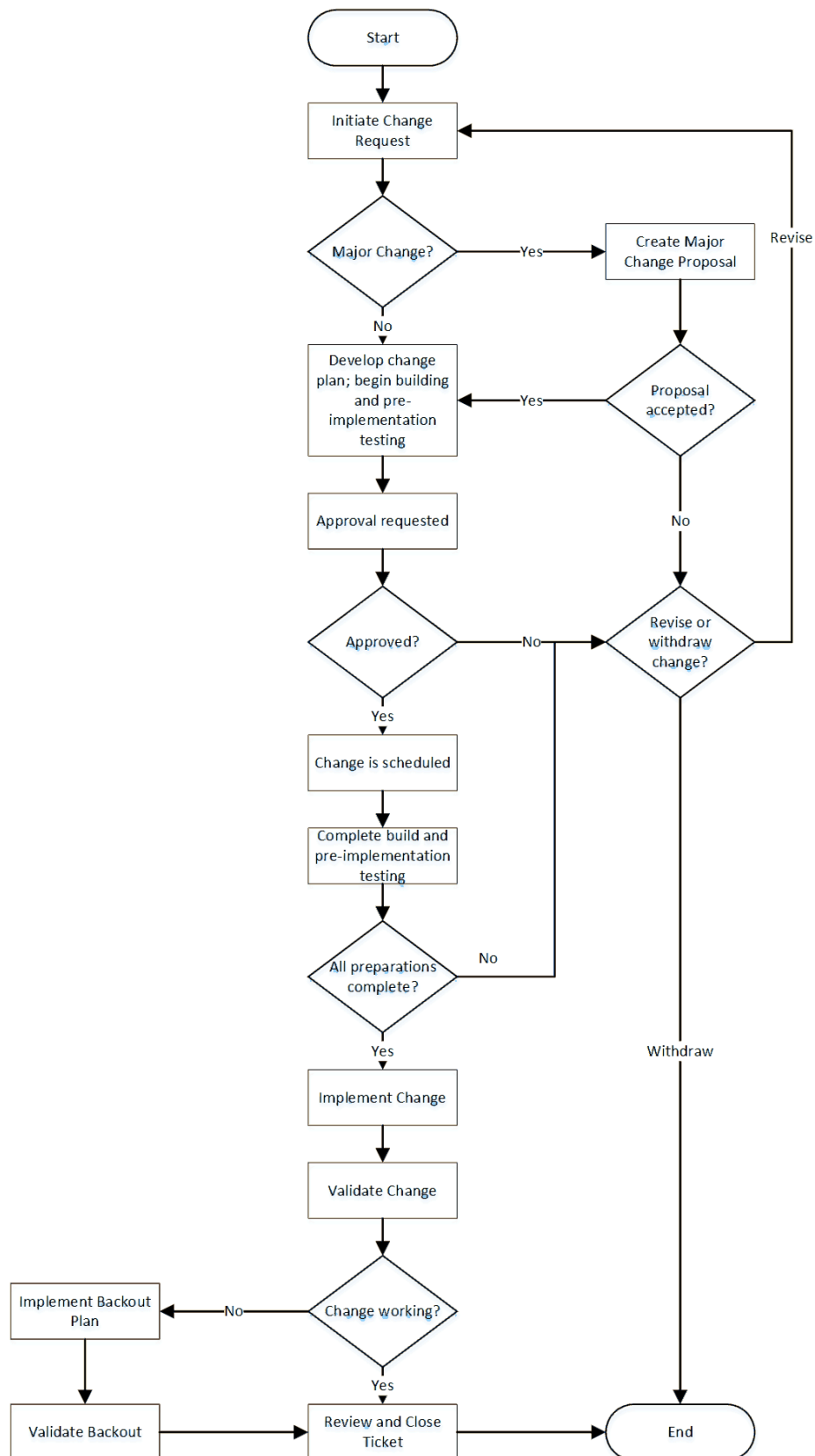
4.2 Change Request Process Activities

4.2.1 Process Flow Charts

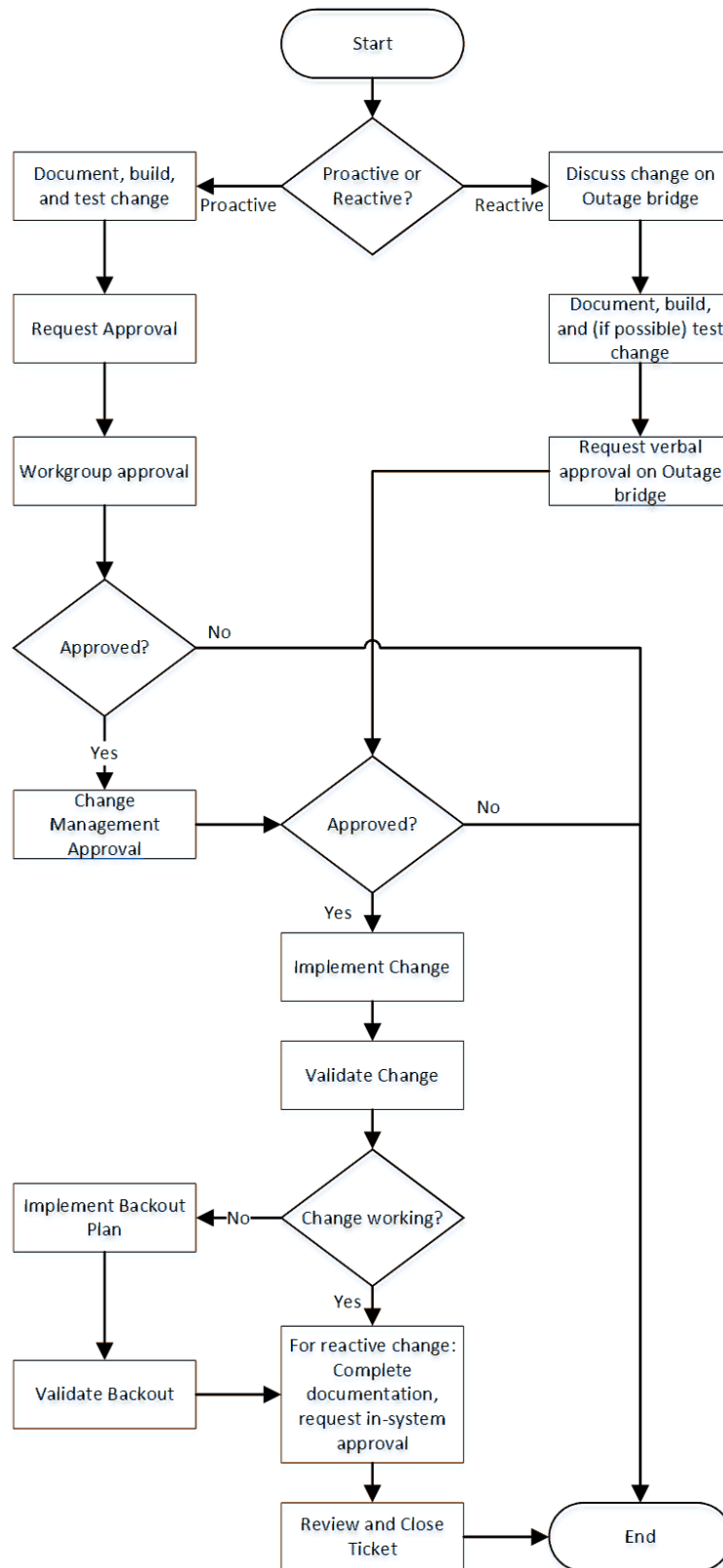
4.2.1.1 Standard Change Request Process Flow



4.2.1.2 Normal Change Request Process Flow



4.2.1.3 Emergency Change Request Process Flow



4.2.2 Planning, Building, and Pre-Implementation Testing

4.2.2.1 Planning and Building

The development of a clear Change Plan is an integral step in the Change Management process, which should be begun even before the Change Request is filed if at all possible. The purpose of the Change Plan is to determine, document, and review the following:

- A high-level Description of the change, including the reasons it is necessary, the expected end state, impact or potential impact on dependent services, any expected service disruption, and planned communication prior, during, or following the change
- The Entities (Configuration Items) that will be affected by the Change Request
- A Change Plan detailing the tasks required to implement the Change Request
- The Impact, Risk, and Planned Implementation Dates
- What testing is being done (or has been done) prior to implementation to ensure that the change plan and change will work as expected
- Means and method for validating that the change was successful
- The Workgroups necessary to implement and validate the Change
- A Backout Plan detailing the tasks required to back out the change if it was not successful (or why backout is not possible)

The Approvers for a given Change Request (local management and CAB) will ask questions and provide input regarding aspects of the Change Plan, and may withhold final approval for a Change pending completion or revision of the Change Plan. At the time a Change Request is submitted, the Plan should be sufficiently developed to identify and document (at a high level) all tasks associated with the Change. Tasks may not be added, deleted or changed after a Change Request has been approved unless doing so reduces the scope of the change without increasing risk or potential impact. If modifications are necessary, the Change Request must be re-submitted through the approval process so the modification can be reviewed and approved at all levels. (Note that any change to the Planned Implementation Date will also require that the Change Request be re-submitted through the approval process.)

The Change Owner, Implementation Manager, and/or Release Coordinator are expected to coordinate with the Service Desk, customers, and groups within IT Services as necessary to ensure that all tasks and Workgroups are correctly identified.

Standard Changes will develop a basic Description and appropriate Change, Test, and Backout plans as part of the package which is submitted to CAB for pre-approval. If, in any given instance of a Standard Change, any aspect of the pre-approved plans does not apply, then that instance cannot be considered a Standard change and must be submitted as a Normal change instead.

4.2.2.2 Pre-Implementation Testing

All Normal and Standard Changes must undergo appropriate testing (where possible) before implementation. Tests should be designed with the following goals in mind:

- Ensuring that the Change can be completed without unexpected disruption to the Service
- Ensuring that the Change accomplishes what it is intended to
- Ensuring that the Change will not have an unexpected negative effect on the Service in terms of performance, stability, or functionality
- Ensuring that the change can be successfully backed out using the documented backout plan

- Ensuring that change implementation, validation, and (if necessary) backout can be accomplished within the requested change window

An overview of pre-implementation testing must be included as part of the Change Request. If, for any reason, it is not possible to fully test a change prior to implementation, this should be explicitly stated (and explained) as part of the Change Request.

If a completed change is selected for audit or review, then that audit will include reviewing what pre-implementation testing was done. The focus will be on any issues that arose during the change implementation itself or as a result of the change and how pre-implementation testing might have prevented those issues. If the change was backed out, then the audit will similarly review whether pre-implementation testing might have prevented the need for reverting the change.

Testing is also encouraged for Emergency changes, but it is understood that, due to the compressed time available for planning these changes, testing may be similarly compressed.

4.2.2.3 Documentation for Configuration Items

Documentation associated with Configuration Items should be updated immediately after the Configuration Item is changed. If the documentation resides on the Configuration Item itself and can be updated at the same time that the Configuration Item is changed, then the update of the documentation should be included in the procedures for the Task that executes the change. Otherwise, a separate “documentation only” Task must be created.

4.2.2.4 Validation & Rollback

Every Change Request must include a validation procedure which is performed once the change is implemented. The purpose of validation is:

- To verify that the change has installed successfully and is working as expected, and
- To verify that the change has not had any unexpected impact on the service or on dependent services (i.e. that the service and dependent services are all functioning normally)

Validation test plans should include explicit standards which define whether a change has been successful, or if it has failed and must be rolled back.

Long, complex changes with many interdependent tasks should contain multiple checkpoints to validate that individual tasks or groups of tasks have completed successfully. This will enable faster response and (if necessary) rollback if an early task fails or has an unexpected impact.

4.2.2.5 Grouped work activities

It is often the case that two or more tasks associated with a Change Request must be executed in the same Change window. Similarly, sometimes one task must be executed before another can begin. When there are multiple tasks for a single Change Request, a detailed plan should be created in order to facilitate proper execution of the entire Change Request. For large-scaled changes involving major application upgrades or large-scale changes to infrastructure, Tasks may be broken up into separate Change Requests and/or coordinated through a full Project Plan.

4.2.3 Initiating a Change Request

In order to initiate a Change Request, the information needed to assess and categorize it must be provided. This includes information regarding the nature of the change, the Change Plan, Impact and Risk assessment, and Planned Implementation Dates. A Change Request cannot be submitted for approval without this

information. It is important to note that submitting a Change Request does not guarantee that a change will ultimately be scheduled and implemented.

The steps for initiating a Change Request include:

- Enter the Change Request into the system
- Assess the accuracy and completeness of the information provided on the Change Request templates
- Determine the Change Type, Risk, and Impact
- Perform supplemental data gathering and analysis deemed necessary in order to evaluate the Change Request

Change requests are made within the ticketing system of record for Change Management (see section 5.1).

It is the responsibility of the person performing a change to decide (using the standards outlined in this document) if a change ticket is required and to make sure it is filed accurately and on time.

If there is any question as to whether a change ticket is required, contact the Change Manager.

The following information should be included in a Change Request where relevant. Some of this information may be requested in explicit fields within the Change Request Management system; other information should be included as part of the Change Description.

- General Change Information
 - Change Description
 - Change Purpose (including reason for the change and how it fits in with any larger project or program)
 - Change Owner
 - Change Requestor
 - Change Request Additional Information
- Scheduling Information
 - Requested Change Implementation Start Date/Time
 - Requested Change Implementation Completion Date/Time
- General Impact and Risk Information
 - IT Services Group(s) executing Change activities
 - Does the Change Request require modifications to operational procedures?
 - Does the Change Request require modifications to Support Procedures?
 - Once implemented, can all Change activities be rolled back completely?
 - What is the practical impact of the change, at a detailed level?
 - What servers/services are affected?
 - What locations on campus are affected?
 - What are the demographics of affected users?
 - What testing is being done prior to implementation to ensure that the change plan works and that the change will perform as expected?
 - Does the Change Request include the addition, deletion, or modification which will be performed? (i.e., detailed description of the exact change)?
 - Does the Change Request include the addition, modification, or deletion of centrally managed backup processes?
 - Will the Change Request cause a measurable change in resource usage of a centrally managed server?
 - Will the Change Request cause a measurable increase in traffic on or a change to computing patterns on the network?

- Will the results of the change be visible to the affected customers?
- Does the change require modification to user procedures?
- What steps are necessary to validate that the change is successful and that services are operating normally?
- What is the communications plan?
- Production Acceptance Information
 - What steps are necessary to validate that the change has completed successfully and is working as expected?
 - What steps are necessary to confirm that the modified service, and any dependent services, are functioning normally?
 - What criteria will be used to determine whether a change has failed and should be backed out?

It is the responsibility of the Change Owner to ensure that the above data is up-to-date throughout the Change Life Cycle.

4.2.4 Approval and Scheduling

The purpose of the Approval and Scheduling phase is to:

- Assess Change Plans for risks, issues, and resource conflicts.
- Ensure appropriate awareness of changes and change impacts among all affected users and groups.
- Ensure that appropriate processes have been followed in determining the need for a change.
- Review the Forward Schedule of Changes to avoid concurrent changes with overlapping impact, or changes which conflict with business events or processes.
- Obtain signoff and approval at the appropriate levels for the change.

Among criteria used to determine whether a Change Request should be approved are:

- Has all information been provided completely and accurately?
- Are there any existing Change Requests that conflict with this Change Request either for resources or because of timing?
- Are there any pre-requisite changes which must be completed before this Change Request?
- If the change will involve an unusual outage or otherwise have a visible impact on end users, is there sufficient lead time to communicate this to the users?

Upon completion of the Approval and Scheduling phase, the Change is returned to the Change Owner for revision or rescheduling if it is not deemed production-ready or if the proposed Date of Change is deemed problematic. The Change Owner may revise the request as appropriate and resubmit the request, or Withdraw the request if the review has made it clear that the request needs more consideration. If Approved, the Change is placed on the Forward Schedule of Changes and is considered Scheduled.

4.2.5 Implementation and Validation

The purpose of the Implementation Phase is to:

- Successfully complete all scheduled Change activities
- Validate that the change was successful, i.e. that the changed configuration item is operating as expected and there have been no unexpected changes in behavior (Incidents) either for this service or dependent/related services
- Execute the Backout Plan if the change is unsuccessful.

The Implementation Manager or Change Owner is accountable for making sure that all activities are completed as planned. In some cases, something unexpected will happen; in this case, the Change Owner or Implementation Manager must determine whether to modify the change plan “on the fly” or cancel the change and back out. This decision should be made in consultation with the Service Owner, who should in turn involve the Business Owner if the modification or cancellation of the plan may have a significant business impact. As a rule of thumb, if the necessary modification is minor – for example, calling in a system administrator to change a file permission, or restarting the service – the change may proceed. More significant modifications to the planned activities, especially those which may lead to an extended unscheduled outage or invalidate pre-implementation testing, should be avoided; in these cases it is preferable to cancel the change and either back out of any work done or (if it’s safe to do so) leave the change only partially completed.

The Implementation Manager or Change Owner should also keep track of the amount of time left in the change window. If the change window begins to run long, and it becomes apparent that there will not be enough time to complete all change activities (including validation testing and, if necessary, backout), the Implementation Manager or Change Owner must escalate to the Service Owner to determine whether it is better to extend the window; execute the backout plan immediately; or leave the change partially completed.

Validation plans should include explicit criteria for determining whether a change has succeeded or failed, and what actions to take in response to any given validation failure (e.g., backing out completely; accepting a service which is not in the desired state but is also not degraded from the user’s purposes; accepting a degraded service for a short period). If validation produces a very unexpected or ambiguous result, especially one which threatens to lead to the change overrunning its scheduled window, then the Implementation Manager or Change Owner should contact the Service Owner or Service Manager to determine how best to proceed.

The Service Owner may establish guidelines for various types of changes (especially Standard Changes) granting the Change Owner authority to extend a change window or modify a change plan in particular circumstances, and at what point they should escalate if a change encounters issues. These guidelines should also address any communication to the business, departments, IT partners, or campus as appropriate.

4.2.6 Closing the Change Request

When the all change activities have been executed, or when it becomes clear that the change cannot be completed successfully in the scheduled window and steps have been taken to guarantee production stability, the Change Owner or Implementation Manager should close the ticket. They should also at that time note any special conditions that occurred during the course of implementation, including

- Any unexpected difficulties that arose
- Any on-the-fly modifications to the change plan
- If the change was not fully completed, what was done or left undone, and why the change could not be completed as planned
- If the change failed, some information about the nature of the failure (e.g. error messages) and an assessment of the system's current state (e.g. whether the backout plan was successfully implemented, or whether there is some residual modification left in place which others should be aware of)
- If no work was done on the change (i.e. the window was missed), information on why the change did not take place as scheduled

A Change Request can also be closed as using the State “Canceled” without detailed comment if it is no longer needed and/or is being delayed indefinitely.

4.2.6.1 Close Codes

A Close Code is assigned according to how successful the change was:

- If all change activities have been executed successfully with no unusual complications or unexpected Incidents, the Close Code is “Successful”.
- If the change has not been implemented successfully, the Close Code is “Unsuccessful”.
- If the change has been partially implemented, or if it was fully implemented but serious complications arose during the process (especially if there are unexpected Incidents), the Close Code is “Successful with Issues”.

Ideally, when a Change is closed as Successful, that means it has caused no unexpected disruptions (Incidents). If a Change causes an incident after implementation, then that indicates a flaw in either the validation plan or the building and pre-implementation testing phase. In either of these cases, a Problem ticket will be raised to identify improved test and validation activities which can prevent these issues in the future.

Note that no Close Code is necessary if a ticket is withdrawn using a State of Canceled.

4.2.6.2 Change Closure Escalations

Change Owners should close Requests promptly when the change implementation is done, whether successful or unsuccessful, ideally before the scheduled end time listed in the Request. If a Change Request in the “Implement” State is not closed by the scheduled end time, the system will send out escalation notifications as follows:

Scheduled End Time Plus...	Notification To...
...One hour	Change Owner
...Six hours	Change Owner, Change Owner’s Manager, Change Manager
...Twelve hours	Change Owner, Change Owner’s Manager, Change Owner’s Director, Change Manager
...24 hours and each 24 hours after until it is closed	Change Owner, Change Owner’s Manager, Change Owner’s Director, Change Manager

4.3 Change Management Administration

4.3.1 Change States

Change Requests move through a number of States between the time the request is created and when it is closed. The Change Management process tracks two states semi-independently of each other, the general Change Request State and the Approval State.

4.3.1.1 Change Request State

Change Requests may move through the following States during their lifetime:

- **New:** All Requests are placed in this State at the time they are created, and remain in this State until Approval is requested, or until the Request is closed if no approval is ever requested. Additionally, at any time before the Request is closed or in a state of Implement or Review, a user can manually return the ticket to the New state (if, for example, it becomes necessary to reschedule the change); doing this will cancel existing approvals and approval requests.
- **Authorize:** When a user requests approval, the system automatically changes the State to Authorize (this State cannot be manually chosen). The Request remains in this State until it is approved, closed, or reset to New. (Note that Standard Changes which do not require Business Approval will normally skip this State.)
- **Scheduled:** When a ticket has received all necessary approvals, the system automatically changes the State to Scheduled (this State cannot be manually chosen). The Request remains in this State until the Planned Start Date on the ticket, or until it is closed or reset to New. Additionally, the system may be configured to prevent modification of some fields to preserve the record of what work was approved.
- **Implement:** When a Scheduled ticket reaches its Planned Start Date, the system automatically changes the State to Implement (this State cannot be manually chosen). The Request remains in this State until it is closed (once a Request reaches this State it can no longer be reset to New). Additionally, the system may be configured to prevent modification of some fields to preserve the record of what work was approved.
- **Review:** All Emergency Changes and Unsuccessful changes must be reviewed by Change Management before they can be closed; accordingly, any Emergency or Unsuccessful Request must be shifted to the Review State from Scheduled, rather than going to Closed. Any user can change to this State from Scheduled, but only the Change Manager can change it from Review to Closed or Canceled. (A Request in this state cannot be reset to New.) Additionally, the system may be configured to prevent modification of some fields to preserve the record of what was done.
- **Closed:** When all work necessary to implement the Change has been completed, the Request State is changed to Closed. Once a Request is in this State, it cannot be changed to any other State. Additionally, the system may be configured to prevent modification of some fields to preserve the record of what was done.
- **Canceled:** Any user can always change a Request to this State, marking the Request as inactive and no longer needed. Once a Request is in this State, it cannot be changed to any other State.

4.3.1.2 Approval States

The current Approval State is tracked independently of the Request State. This allows unapproved Changes to be properly recorded, while maintaining a record that the Change was not properly approved. The Approval States are:

- **Not Requested:** Approval has not yet been requested. This is the default Approval State when a Request is created. Additionally, whenever a Request is reset to a State of “New”, the Approval State will be reset to Not Yet Requested, and all existing approvals and outstanding approval requests are canceled. In effect, this Approval State should always correspond with a State of New (unless the Request is Closed or Canceled without approval having ever been requested).
- **Requested:** When a user Requests Approval for a Request, the system automatically adjusts the Approval State to Requested. In effect, this Approval State should always correspond with a State of Authorize (unless the Request is Closed or Canceled without full approval having happened).
- **Approved:** Once all relevant approvals have been given, the Approval State is automatically changed to Approved (at the same time that the State is changed to Scheduled).

Note that Approval State can never be manually modified.

4.3.2 Review and Approval Bodies

4.3.2.1 QA Lite

The purpose of QA Lite is as follows:

- To review changes to financially significant applications prior to CAB review in order to approve the planning or provide input as necessary.
- Evaluate the business impacts of these changes.
- Ensure changes are assigned proper change request levels.
- Ensure that the change receives appropriate approval from the business.
- Confirm that changes are properly tested before production deployments.
- Confirm documented practice for separation of duties between development and deployment.

This additional level of scrutiny by staff and management intimately familiar with the business processes involved helps ensure that correct audit control standards are being met for these applications.

The QA Lite review process is run under the auspices of the ITS Change Management Framework and adheres to the standards of this framework, but maintains an independent charter and membership from CAB to meet audit standards. The Change Manager is an ex officio member of QA Lite to ensure that standards and coordination are maintained between CAB and QA Lite.

4.3.2.2 Change Advisory Board (CAB)

The purpose of the Change Advisory Board (CAB) includes:

- Reviewing Change Plans in order to approve the planning or provide input as necessary.
- Review Emergency and Unsuccessful changes post-implementation for lessons learned and opportunities for process improvement.
- Review and discuss unauthorized, implemented changes.
- Discussion and approval of changes to be assessed and/or implemented.
- To review Change Requests for approval in order to schedule and finalize resources for the change activities associated with them.

The CAB meeting is held under the direction of the Change Manager according to a schedule set by the Change Manager in consultation with CAB members (at minimum once per week). The Change Manager sets the agenda, facilitates the meeting, and documents the results of the meeting.

All of the major operational and application areas are expected to appoint standing CAB members who will attend all CAB Meetings. Change Owners attend all meetings at which their change is discussed. The Change Manager may invite additional participants (e.g. Subject Matter Experts, Managers, Liaisons, IT partners, business area representatives) if such an invitation seems appropriate (for example, if this would help CAB understand the business impact of a particular change).

The Change Manager will define how far in advance changes must be submitted to CAB for approval. Changes which are submitted to CAB without sufficient lead time will be deemed Out of Process. The Change Manager has the authority to reject Out of Process changes unilaterally if there is no customer-driven reason for the late status.

4.3.2.3 Emergency Change Advisory Board (ECAB)

Proactive Emergency changes often arise suddenly and require rapid response to prevent a service disruption. Such a change may need to be applied before the next regular CAB meeting. In these situations, the Change Manager will normally ask the CAB for an ad hoc review by email. If this is unrealistic – for example, if a situation arises late in the day which must be addressed overnight – the Change Manager will convene and Emergency Change Advisory Board (ECAB). The ECAB is an ad hoc group consisting of the Change Manager, the Service Owner and Service Manager of the service being changed, senior IT leadership over areas affected by the change, and such other managers, technicians, and subject matter experts as the Change Manager deems necessary. This group will review and approve (or reject) the change using the same criteria as the regular CAB, taking into account the constraints and time pressures involved in responding to a critical situation.

Reactive Emergency changes are applied in response to an ongoing Incident, often a Major Outage. In these circumstances, a technician may proceed with the change on verbal approval from the Service Owner, Service Manager, and/or Change Manager (for example, on an Outage Bridge), and create a Change Request documenting what was done after the Incident is resolved. This must be done within one business day of the change, and the Change Request must still receive ex post facto Workgroup and Change Management approval asserting that the change was approved and that the documentation is complete.

4.3.2.4 Appeals and Approval Escalation

The Change Manager has the authority to establish rules of protocol governing what constitutes a valid approval within CAB (e.g. general vote, consensus, what constitutes a quorum, etc.) to reflect the current structure and priorities of the IT Services organization.

In general, CAB and Change Management approval are considered final. If a Service Owner feels that a given change has been approved or rejected inappropriately, they may appeal to the Change Manager to conduct a second review and either re-affirm or overturn the previous decision. If the Service Owner is still unsatisfied, the next level of appeal is to the ITS Senior Leadership Group. The Change Manager or CAB may also choose to escalate approval for a given change to ITS Senior Leadership if they feel that there are conflicting priorities or political concerns which require a higher level of review.

4.3.3 Review of Completed Changes

4.3.3.1 Review of Unsuccessful and Emergency Changes

All Unsuccessful and Emergency changes will be reviewed by CAB within one week after the change is closed. These reviews will take place during a normal CAB meeting. The purpose of these reviews is to improve the overall change implementation process. This is accomplished by:

- Determining why changes succeed or fail
- Making recommendations to the Change Management team and project teams for general process improvements
- Making recommendations to Service Managers, Subject Matter Experts, Implementers, etc. for specific change-related process improvements

It should be noted that the intent of reviewing an unsuccessful or Emergency change is not to place blame, but to identify general and procedural issues that can be corrected in the future.

4.3.3.2 Audit of Standard Changes

The Change Manager will, on a monthly basis, convene a group consisting of Change Advisory Board and QA Lite members to audit a random sample of Standard changes performed during the previous month, as well as a random sample of low-risk/low-impact Normal changes which were not reviewed by CAB. The goal of this audit will be to ensure that these changes were assessed at the correct risk and impact, and also confirm that the changes underwent (and documented) appropriate testing, approval, and implementation processes.

4.3.3.3 Other Reviews and Audits

In addition to the above, the Change Manager, Configuration Item Owner, Customer, Service Owner, Service Manager, or any member of an Implementation Team may request that a specific Change Request be reviewed. In most cases, these reviews will be intended to bring forth a specific problem or issue for discussion. All change reviews should be arranged through the Change Manager, who will ask CAB to review the change or arrange a separate meeting with the relevant people as seems appropriate. If a separate review is deemed necessary, the results of the review will still be documented and submitted to CAB for informational purposes.

4.3.4 Maintenance Windows and Blackouts

4.3.4.1 Standard Maintenance Window

Each Service is expected to negotiate a Standard Maintenance Window with the Business Owner for that service as part of its Service Level Agreement. Standard Maintenance Windows should always be set outside peak usage hours. In cases where Standard Maintenance Windows for technical/infrastructure services conflict with the Standard Maintenance Window for a user-facing service, the latter should be preferred; if multiple Standard Maintenance Windows are in conflict, then an appropriate maintenance window should be negotiated as part of the Change Planning Process.

During a service's standard maintenance window, users should neither expect nor plan on system availability because IT Services systems and services may be implementing an approved change. However, Service Owners may still wish to communicate changes, particularly if the change is disruptive or if the service does not frequently utilize the Standard Maintenance Window.

Non-Emergency changes scheduled outside of a Standard Maintenance Window must have explicit approval from the business for the exception. Even with this approval, CAB may still give preference to a change taking place during its Standard Maintenance Window over an exception, if there are conflicts.

4.3.4.2 Change Blackouts

The Change Advisory Board maintains a standard change blackout at the beginning of each academic quarter. During these blackouts Normal changes cannot be implemented, and Standard and Emergency changes receive extra scrutiny. As a general rule these blackouts will be:

- For Autumn Quarter: From 6 a.m. on the Friday prior to Orientation Week through 10 p.m. of First Week
- For Winter and Spring Quarters: From 6 a.m. on the Friday prior to First Week through 10 p.m. of First Week

These windows may be extended occasionally based on the exact starting dates for a given quarter.

CAB may also recommend a change blackout be imposed at other times. Among the reasons for additional Change Blackouts are:

- Critical processing or business events that cannot be interrupted are taking place.
- A critical application or new technology is being implemented
- A large problem has surfaced and the blackout is needed in order to determine the problem's cause and resolution.

Additionally, Service Owners are always free to declare change freezes for their service(s) based on business or organizational needs. In this circumstance, the Change Advisory Board will work with the Service Owner to identify and remediate changes which would affect the frozen service.

4.3.4.6 Emergency Change Requests

If Change activities associated with an Emergency Change Request are being planned and scheduled at a CAB meeting, the Change Manager is responsible for noting all commitments and conflicts.

It is possible for change activities associated with an Emergency Change Request to pre-empt other scheduled changes. Should these conflicts occur the Change Manager will notify all persons affected by the scheduling change. The Change Manager may choose to organize a special CAB meeting to reschedule pre-empted activities.

4.3.5 Defining and Documenting Standard Changes

Changes that are low-risk, low-impact, common, and use the same, repeatable procedure in every instance can be classified as Standard Changes. Standard Changes are still documented in the ticketing system of record, but have reduced approval requirements, typically only requiring workgroup approval (and business approval, in the case of financially significant applications). Examples of Standard Changes might include simple configuration changes using a standard application interface, manually applying system patches to non-critical servers, or updating expiring licenses or SSL certificates.

In order to have a change classified as Standard, the Service Owner or Service Manager must assemble documentation for the change which includes:

- Short change name
- Short description for the change
- Description of any likely impact that the change could have, either expected or unexpected

- Step-by-step plan for implementing the change
- Step-by-step plan for validating the change
- Step-by-step plan for backing the change out if it fails validation
- A description of when the change is performed, including the circumstances (e.g. per customer request, when a new patch is released) and what time of day it can take place in (e.g. only during standard maintenance window, outside business hours, etc.)
- Required approvals per instance (no approval or workgroup approval; business approval will always be required for financially significant changes)

This documentation will be submitted to the Change Manager via a Normal Change Request. The Change Manager will review it for completeness, clarity, and precedent. Once the Change Manager is satisfied, the documentation is submitted to CAB for review. If CAB agrees, the change is declared Standard; otherwise it must continue to be submitted as a Normal change. (CAB may also suggest that the change might be more suitable as a service request or a documented maintenance activity rather than a change.)

Three things to keep in mind regarding Standard Changes:

- The Service Manager should review documentation for Standard Changes whenever there is a major upgrade or significant evolution of the Service. If steps have changed for implementation, validation, or backing out, or if the expected impact has changed, then the documentation must be updated and resubmitted to CAB for re-approval.
- If the authorized plan for a Standard Change does not apply in a given instance – for example, if a specific application configuration update would require restarting the service, but a service restart is not included in the standard implementation plan – then that instance cannot be considered Standard, and must be submitted as a Normal change.
- If a Standard Change causes a Major Incident, or frequently causes minor incidents, then the Change Manager has the authority to revoke the Standard classification and require that such changes be submitted as Normal until the underlying problem has been resolved.

4.3.5.1 Maintenance Activities vs. Standard Changes

Technicians regularly perform a wide variety of activities as day-to-day operational maintenance of a service. Examples might include clearing caches and temp files, growing available disk on a server, or closing and clearing out unused accounts. These activities may be performed during scheduled maintenance periods or as necessary when a technician notices a potential issue. As with Standard Changes, all maintenance activities should be documented and submitted for CAB review; if CAB agrees, then these activities will not be classified as changes, and will not need to be tracked by tickets. Also as with Standard Changes, if a given maintenance activity causes a major outage or frequently causes minor incidents, then the Change Manager has the authority to revoke its status as a maintenance activity and require that these activities be submitted as Normal changes until the underlying Problem has been resolved.

4.4 Relationship to Other ITSM Processes

4.4.1 Service Request Management

Many (if not most) Service Requests are low-risk, low-impact activities which are being performed at user request. Technically these could be defined as Standard Changes, but practically speaking, that would usually be redundant for tracking purposes.

In other cases, however, the Service Request process is used to collect requests for higher-risk changes that do require a Change ticket to create a clear, common record of when the change occurred in the context of other changes. An example would be firewall rule updates. In this case, both a Service Request and a Change ticket are required, and the two should be tied together in an appropriate manner.

In order to ensure that Service Requests do not pose any conflict with Change Management, the Change Manager participates in the review of specific Service Request processes as they are submitted by Service Owners.

4.4.2 Incident Management

Changes are one of the primary cause of Incidents, and it is not uncommon that incidents require changes to restore normal service. Service Owners are accountable for ensuring that all changes which cause incidents to their services are appropriately linked to those incidents in the ticketing system of records. Service Owners are also accountable for ensuring that all changes which resolve incidents are appropriately linked.

4.4.3 Outage Management

Outage Management is one of the major processes which lead to reactive Emergency Changes. If it is determined during the course of an outage that an Emergency Change may be called for, then the Outage Coordinator, Service Owner, and Service Manager may be considered an Emergency CAB for approval purposes, or (if there are concerns about possible cascade effects) they may call on the Change Manager to convene a broader ECAB. The Service Owner is accountable for ensuring that a technician enters an Emergency Change into the ticketing system of record within one business day of its implementation, and for ensuring that this change is then tied into Incident and Problem records as appropriate.

4.4.4 Problem Management

Permanent resolution of a Problem will often require one or more changes to the affected Service. The Service Owner is accountable for ensuring that any changes performed to resolve a Problem are appropriately tied to the Problem record. Similarly, in some cases a flaw in a change implementation plan, or a problem with the change itself which was not caught during pre-implementation testing, may be the root cause of a Problem; these changes must also be tied to the Problem record.

Note that all changes which were closed as Complete or Incomplete which cause Incidents must have a Problem raised to identify improvements in pre-implementation testing or validation which will prevent similar incidents in the future.

4.5 Metrics

The Change Manager will periodically distribute the Change Metrics report. This report summarizes CAB activity, as well as providing information about how successfully IT Services is able to plan successful changes. Metrics include:

- Number of changes approved
- Number of changes implemented without approval
- Number of changes that cause incidents
- Number of changes that raised problems (by causing unexpected incidents after the change was marked complete)
- Number of changes completed successfully and unsuccessfully
- Number of emergency and out-of-process changes

This list is not comprehensive; other metrics may be added or removed as needs are identified. Metrics are distributed to service managers, service owners, and operational and senior leadership in ITS. Service-specific metrics may also be distributed to business owners on request.

5.0 Communications

5.1 Ticketing and Systems of Record

All changes within the scope of the Change Management Process must be documented and tracked in the ITS ticketing system of record, which at the time of this writing is ServiceNow:

<https://uchicago.service-now.com/>

In some cases, the working relationship between ITS and specific customer groups may lead to Changes which arise from incidents, service requests, or requests for change filed in a ticketing system other than ServiceNow. In such cases, the ServiceNow ticket must contain information about the original ticket, as follows:

- If the original ticket is reasonably short and clearly contains all the information describing the change, then it can be copied and pasted into the Description field of the ServiceNow ticket, along with the name of the original ticketing system and the ticket number in that system.
- If the original ticket is complex, or if the nature of the change is not immediately obvious from the content of the original ticket, then a PDF copy of the original ticket should be attached to the ServiceNow ticket. The Description should still contain the name of the original ticketing system and the ticket number in that system.

If a large number of tickets are being bundled into a single change (e.g. a number of requests for change bundled into a single release), it is acceptable to create a document listing the ticketing system of origin, original ticket number, and a short description of the ticket, for each ticket bundled into the change, and attach that spreadsheet to the ServiceNow ticket.

5.2 Internal Communications

5.2.1 CAB Minutes and Reviews

The Change Manager is responsible for publishing the minutes to all CAB meetings, and notes for any post-implementation change reviews which occurred outside of CAB, within three business days of the meeting or review in question. These documents will be kept in a central ITS document repository available to all ITS staff. The Change Manager may also maintain mailing lists or instant message channels to communicate the release of CAB minutes and agendas to those members of ITS who are interested.

5.2.2 Forward Schedule of Change

The Forward Schedule of Change contains execution dates and times for requested and approved changes. The Change Manager is accountable for ensuring that the Forward Schedule of Change is current and accurate. This schedule will reside within the ServiceNow system.

5.2.3 System Notifications

The ticketing system of record will send out regular email notifications regarding the status of change tickets in the system. Specific notifications will be developed by the Change Manager in consultation with CAB members, but at minimum will include:

- Notification to assignment groups when a change is assigned to them
- Notification to assignees when a change is assigned to them
- Notification to approvers when their approval is requested

- Notification to approvers and Change Management when approvers have not responded in a reasonable period of time
- Notification to ticket assignee, assignment group management, and Change Management when an approved ticket is not closed promptly after the change's scheduled end date
- Notification to ticket assignee and assignment group management when a change is closed
- Notification to Change Management when an Emergency change is created

The Change Manager is responsible for reviewing notifications on an annual basis to ensure that an optimal set of notifications is being maintained and that the text included in notifications is useful and appropriate to the notification.

5.3 External Communications

5.3.1 Coordinating with Customers

Changes to services closely affiliated with a single business process (for example, financial or student systems) must often be coordinated with the business owner to ensure they do not interfere with critical business events. This is especially important when the change will be very disruptive (require extensive downtime or result in major transformation of the user experience). In these situations, the Service Owner is accountable for working with the business and with Change Management to identify and agree on a date for the change, keeping in mind the necessary lead time for changes which need to go before CAB.

Service Owners are encouraged to negotiate standard change windows for their services when scheduled outages can occur, to simplify this process.

5.3.2 Customer and Campus Notification

Customer notification of major tested maintenance and emergency changes should be provided within the parameters identified in Change Type table above.

For changes which affect only a small number of users (for example, a single department), this notification will be written and sent by appropriate IT Services staff members. For changes affecting multiple departments, the Change Plan should incorporate Liaisons and IT Services Communications into the process as appropriate, to ensure that all customers are sent a consistent message without being “over-notified”. During its review, CAB may suggest additional parties to be communicated or coordinated with.

All change notifications should be considered an important opportunity to communicate with customers and be presented with the most relevant impact, cause, and benefit information available – customers appreciate full understanding of changes.