### Document Change Control

<table>
<thead>
<tr>
<th>Version #</th>
<th>Date of Issue</th>
<th>Author(s)</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3/8/13</td>
<td>J.Worthington</td>
<td>Initial Draft</td>
</tr>
<tr>
<td>2.0</td>
<td>3/25/13</td>
<td>J.Worthington</td>
<td>R.Lo review and edit. Submit to core team for review.</td>
</tr>
<tr>
<td>3.0</td>
<td>4/5/13</td>
<td>J.Worthington</td>
<td>Ready for CAB Review</td>
</tr>
<tr>
<td>3.1</td>
<td>4/9/13</td>
<td>B. Leishman</td>
<td>Clarified scope of configuration management integration</td>
</tr>
<tr>
<td>4.0</td>
<td>4/18/13</td>
<td>B. Leishman</td>
<td>Incorporated CAB feedback &amp; updated Risk matrix</td>
</tr>
<tr>
<td>5.0</td>
<td>10/1/15</td>
<td>B. Leishman</td>
<td>Updated to reflect iterative process improvements</td>
</tr>
</tbody>
</table>

*Table 1 - Document Change Control*
# Table of Contents

Document Change Control ............................................................................................................................................. 2

1. **Introduction** .......................................................................................................................................................... 5

2. **Objectives & Scope** .............................................................................................................................................. 5
   2.1. **Objectives** ..................................................................................................................................................... 5
   2.2. **Scope** ............................................................................................................................................................ 5
       2.2.1. **Out of Scope** ........................................................................................................................................ 6

3. **Types of Changes** ................................................................................................................................................. 7
   3.1. **Risk Assessment** ........................................................................................................................................... 7
   3.2. **Urgency & Change Lead Times** ................................................................................................................... 8

4. **Change Scheduling** .............................................................................................................................................. 10
   4.1. **Change Request Calendar** .......................................................................................................................... 10
   4.2. **Standard Maintenance Windows** ............................................................................................................... 10
   4.3. **Service-Specific Maintenance Windows** ................................................................................................... 10
   4.4. **Major Maintenance Windows** ................................................................................................................... 10
       4.4.1. **Approval and Communication** ........................................................................................................ 11
   4.5. **Business Events** ........................................................................................................................................ 11
       4.5.1. **Change Freeze** ................................................................................................................................... 11
       4.5.2. **Heightened Sensitivity** .................................................................................................................... 12

5. **Process Flow** ....................................................................................................................................................... 13
   5.1. **Standard Changes** ........................................................................................................................................ 16
       5.1.1. **Normal Changes** ................................................................................................................................ 17
       5.2. **Emergency Changes** ............................................................................................................................ 19
       5.3. **Major Changes** ........................................................................................................................................ 20

6. **Roles & Responsibilities** ....................................................................................................................................... 21
   6.1. **Change Requester** ...................................................................................................................................... 21
   6.2. **Implementer/Assignee** ............................................................................................................................... 21
   6.3. **Assignment Group Approver** ...................................................................................................................... 21
   6.4. **Change Approver for Impacted Services** ................................................................................................... 21
   6.5. **CAB Member** ............................................................................................................................................... 21
   6.6. **Change Manager** ....................................................................................................................................... 21
   6.7. **Process Owner** ........................................................................................................................................... 22

7. **CAB Membership & CAB Meetings** .................................................................................................................. 23
   7.1. **CAB Membership** ..................................................................................................................................... 23
       7.1.1. **HUIT CAB Makeup** .......................................................................................................................... 23
       7.1.2. **Functions** ........................................................................................................................................... 23
       7.1.3. **Member Expectations** .................................................................................................................... 23
1. Introduction

This document describes the Change Management process used by HUIT. It is based on the Information Technology Infrastructure Library® (ITIL) and adapted to address HUIT’s specific requirements. This document is divided into the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives &amp; Scope</td>
<td>Specifies the objectives of the Change Management process and what types of changes are “in scope” of the Change Management process versus “out of scope” relative to the Change Management process.</td>
</tr>
<tr>
<td>Types of Changes</td>
<td>Changes are categorized into different types based on risk. Changes with a higher risk level follow a more robust approval process.</td>
</tr>
<tr>
<td>Process Flow</td>
<td>Diagrams illustrating the high-level Change Management process. In particular the following scenarios are covered:</td>
</tr>
<tr>
<td>Roles &amp; Responsibilities</td>
<td>Identifies the roles within the Change Management process and the responsibilities for each role.</td>
</tr>
<tr>
<td>Change Management Policies</td>
<td>Policies that support the Change Management process</td>
</tr>
<tr>
<td>Change State and Approval</td>
<td>Relationship between Change Record statuses and Approval statuses.</td>
</tr>
<tr>
<td>Statuses</td>
<td></td>
</tr>
<tr>
<td>CAB Membership &amp; CAB Meetings</td>
<td>Describes who should be a member of the Change Advisory Board (CAB) and the agenda for CAB meetings.</td>
</tr>
<tr>
<td>Information in the Change Record</td>
<td>Identifies the data elements in the Change Record that will be captured at various stages through the Change lifecycle.</td>
</tr>
<tr>
<td>Key Performance Indicators</td>
<td>Specifies the metrics for measuring the success of the Change Management Process</td>
</tr>
<tr>
<td>Notifications</td>
<td>Service-Now email triggers.</td>
</tr>
</tbody>
</table>

Table 2 - Sections in this document

2. Objectives & Scope

The purpose of Change Management is to allow HUIT to respond to Harvard’s changing business and IT needs while maximizing service value and reducing incidents, disruption and re-work. Change Management achieves this by having standardized methods and procedures for the efficient and effective handling of all changes. These methods include recording all changes and then evaluating, authorizing, prioritizing, planning, communicating, ensuring the testing and documentation, implementing, and reviewing changes in a controlled manner.

2.1. Objectives

The specific objectives of Change Management at HUIT are:

- Establish a standardized process and tool for managing changes
- Right-size the approval requirements based on the level of risk
- Ensure appropriate communications regarding changes, including visibility into the Change Calendar
- Capture metrics and lessons learned to continuously improve the Change Management process

2.2. Scope

The Change Management process will begin when the customer, business, project management, or IT management authorizes the change for development or planning (as opposed to just before the change is about to be implemented). Requesting approval for changes early provides for:

- Better governance, prioritization and planning of work
Early impact analysis avoids delays and rework
Increases Change Calendar visibility
Allows for improved communications

The following activity is **in-scope** of the Change Management process:
- Addition, modification, or removal of production HUIT services or supporting infrastructure
- Addition, modification, or removal of any development, test, and production configuration items contained within the Configuration Management Database (CMDB)

### 2.2.1 Out of Scope

The following activity is **out-of-scope** of the Change Management process:
- Service Requests (password resets, user account setup or modification, new report creation, web or database content updates, etc.)
- Support requests (Incident Management)
- Changes to individual desktop environments
- Changes to non-production infrastructure or applications that are NOT contained within the CMDB
3. Types of Changes
There are four main types of changes:

<table>
<thead>
<tr>
<th>Type of Change</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Change</td>
<td>A low risk, frequently occurring, routine change that has a pre-approved Standard Operating Procedure (SOP).</td>
</tr>
<tr>
<td>Normal Change</td>
<td>A change that follows the normal process flow that may require explicit approval by Group Managers, Service Owners, the Change Manager or the Change Advisory Board (CAB). Normal Changes are further categorized into low, medium or high risk. Please refer to the Risk Questionnaire below for determining the level of risk.</td>
</tr>
<tr>
<td>Emergency Change</td>
<td>A change to resolve an outage or a pending outage or to address a security or regulatory issue. The technical Group Manager must approve emergency changes, either tacitly or explicitly, and confirm signoff from impacted Service Owners as necessary. The change is often recorded after the implementation has been completed.</td>
</tr>
<tr>
<td>Major Change</td>
<td>A change with sufficient institution-wide impact or risk that Senior Leadership Team sign-off and an increased lead-time for submission to the CAB are warranted.</td>
</tr>
</tbody>
</table>

**Criteria**
- Extended interruption of critical services
- Datacenter work that will interrupt most services
- Increased risk to institutional reputation

**Requirements**
- Peer review
- SLT review
- Minimum 6-week advance CAB notice
- Enhanced communications plan
- Schedule during established major maintenance windows

Table 3 - Types of Changes

3.1. Risk Assessment
Normal Changes are further categorized into low, medium or high risk. The risk questionnaire will be based on this matrix, with each change request being assessed based on its Scope, Impact, and Probability of Success:

<table>
<thead>
<tr>
<th>Question</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SCOPE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A measure of the number and relative importance of the services that depend on the item(s) being changed, with consideration given to timing and usage patterns, where applicable.</td>
<td>Services impacted are internal to HUIT, are minor, or have few users.</td>
<td>One or more customer-facing HUIT services</td>
<td>One or more critical HUIT services</td>
</tr>
</tbody>
</table>
2. IMPACT
A measure of two things:
   a) The degree to which services will be interrupted during implementation of the change, or may be interrupted should the change implementation fail (worst-case scenario).

   Change will be transparent to users or will occur during a customer-agreed maintenance window.

   Interruption exceeds any agreed-upon maintenance window, or significant user intervention will be required in order to continue using the service after implementation.

   b) The degree to which the user experience is changed after the change is implemented.

3. PROBABILITY OF SUCCESS
A measure of how well tested the change is or our history of success with similar changes.

   A history of success has not been established AND the change was not successfully tested in an adequate test environment.

   Change is either well tested in an adequate test environment OR a history of success has been well established.

Table 4 - Risk Questionnaire

<table>
<thead>
<tr>
<th>SCOPE</th>
<th>HIGH</th>
<th>MEDIUM</th>
<th>LOW</th>
<th>HIGH/LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>High Risk</td>
<td>Medium Risk</td>
<td>Medium Risk</td>
<td>Low Risk</td>
</tr>
<tr>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Low Risk</td>
<td>Low/HIGH</td>
</tr>
</tbody>
</table>

IMPACT / PROBABILITY

3.2. Urgency & Change Lead Times
The following table specifies the suggested minimum lead-time for submitting the change and the approval process.

Note: the change should be submitted as soon as the customer, business, project or IT management authorizes the change, which typically should be well in advance of the minimum lead-time.

<table>
<thead>
<tr>
<th>Type of Change</th>
<th>Submission Lead Time</th>
<th>Approval Process</th>
<th>How to find out what needs approval?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Same day</td>
<td>Standard changes are pre-approved by the CAB.</td>
<td>Pre-approved</td>
</tr>
<tr>
<td>Normal – Low Risk</td>
<td>1 business day</td>
<td>Assignment Group Approver</td>
<td>Email sent to Approver(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Change Approver for the services impacted by the Change, as necessary. (Each service owner team can specify whether the service will or will not have an approver for low risk changes.)</td>
<td>Approver’s ServiceNow home page contains a gauge listing changes they need to approve.</td>
</tr>
<tr>
<td>Normal – Medium Risk</td>
<td>1 week</td>
<td>Assignment Group Approver</td>
<td>Email sent to Approver(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Others as requested by Assignment Manager and/or Requester</td>
<td>Email sent to CAB Members.</td>
</tr>
<tr>
<td>Type</td>
<td>Lead Time</td>
<td>Change Approver</td>
<td>Other Approvers</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Normal – High Risk</td>
<td>2 weeks</td>
<td>Change Approver for the services impacted by the Change, as necessary. (Each service owner team can specify whether the service will or will not have an approver for medium risk changes.)&lt;br&gt;Others as requested by Assignment Manager and/or Requester&lt;br&gt;CAB approvals via the ServiceNow tool.</td>
<td>Approver’s and CAB Member’s ServiceNow home page contains a gauge listing the changes they need to approve.</td>
</tr>
<tr>
<td>Major Change</td>
<td>6 weeks</td>
<td>IT Leadership identifies a major change, and sends Change proposal to the Change Manager&lt;br&gt;The Change Manager adds the Change proposal to the next scheduled CAB meeting for review</td>
<td></td>
</tr>
<tr>
<td>Emergency Change</td>
<td>N/A</td>
<td>Emergency changes require explicit manager and Emergency CAB (ECAB) review and approval, time permitting. For emergency changes requiring immediate after-hours implementation, explicit ECAB approval is not required.</td>
<td>Verbal/email/text approval by Assignment Group Approver. Change record is created after the fact.</td>
</tr>
</tbody>
</table>
4. Change Scheduling

4.1. Change Request Calendar
All business events and approved changes are displayed in the HUIT Change Calendar, which is available in ServiceNow.

4.2. Standard Maintenance Windows
Standard maintenance windows are a predetermined period of time during which HUIT and partnering organizations can reasonably perform proactive maintenance and enhancements to the IT environment. Whenever possible, standard maintenance windows should be defined on a per-service basis, with consideration given to factors including (but not limited to) criticality of the service, customer type (faculty, staff, student), and existing Service Level Agreements (SLA).

All medium- and high-risk Normal changes should be performed within these windows unless mitigating circumstances require alternate scheduling (i.e. Emergency changes). Standard and low-risk changes are not subject to these scheduling restrictions.

Standard maintenance windows will be used on an “as needed” basis and the external notifications of these activities will occur via email or web posting as designated by our existing communications processes.

In the absence of service-specific maintenance windows, these default standard maintenance windows apply to all services:

1. 8:00pm Tue – 8:00am Wed
2. 8:00pm Wed – 8:00am Thu
3. 8:00pm Thu – 8:00am Fri
4. 5:00am Sat – 12:00pm Sun

4.3. Service-Specific Maintenance Windows
A list of service-specific maintenance windows is maintained on the Change Management page of the HUIT web site at http://huit.harvard.edu/itsm. Unless otherwise noted, these timeframes are in addition to the general timeframes listed above.

4.4. Major Maintenance Windows
Major changes are changes with sufficient institution-wide impact or risk that Senior Leadership Team sign-off and an increased lead-time for submission to the CAB are warranted. To accommodate the scheduling of these high-impact / high-risk changes, 4 major maintenance windows have been identified throughout the year:

Severity 3 Maintenance: This is a six-hour maintenance window. It occurs twice during the year, once in the Fall Semester and once in the Spring Semester. The fall window would be the first weekend after Columbus Day. The spring window would be the first weekend of Harvard’s Spring Recess.

Severity 2 Maintenance: This is a twelve-hour window. It occurs once during the year in the winter. The date is the second weekend after the observance of New Year’s Day. The Saturday of this weekend is reserved for annual data-center power and facilities testing (non-disruptive).

Severity 1 Maintenance: This is an eighteen-hour window. It occurs once during the year in the summer. The date is the second weekend in June.
4.4.1. Approval and Communication
The Change Advisory Board will have the authority to approve requests to use a particular major maintenance window. Communication of which services will be affected during a particular window needs to go out to customers or end-users at least two weeks before the window.

4.5. Business Events
To ensure the availability of services when they are most critical, the HUIT Change Management process adheres closely to the FAS academic calendar. Time periods corresponding to certain business events on the calendar have been classified as either “Change Freeze” or “Heightened Sensitivity”. Unless otherwise noted for specific services, these time periods supersede any regular maintenance windows.

4.5.1. Change Freeze
All term startups are classified as Change Freeze periods, during which additional change restrictions and approval requirements are in place.

<table>
<thead>
<tr>
<th>Business Event</th>
<th>Event Duration</th>
<th>Event Start</th>
<th>Event End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall Term Startup</td>
<td>4 weeks</td>
<td>Monday 2 weeks prior to first week of classes</td>
<td>Friday 1 week after first week of classes</td>
</tr>
<tr>
<td>Spring Term Startup</td>
<td>2 weeks</td>
<td>Monday 1 week prior to first week of classes</td>
<td>Friday of first week of classes</td>
</tr>
<tr>
<td>Summer Term Startup</td>
<td>2 weeks</td>
<td>Monday before move-in weekend</td>
<td>Friday of first week of classes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Table 6 – Change Freeze Periods</td>
<td></td>
</tr>
</tbody>
</table>

4.5.1.1. Restrictions
No medium or high risk changes to critical services or major project deployments should occur during this time period. Exceptions require Senior Leadership Team (SLT) approval. See below for requirements. Any low risk changes that impact critical services should receive additional scrutiny, with the change presented to the Change Advisory Board (CAB) for review as necessary.

4.5.1.2. SLT Exception Requirements
Requests for exceptions to the above restrictions during term startup events should be made in writing via email to the SLT Exception Committee and should address the following concerns:

- Business risk (i.e.: What is the risk of implementing now vs. waiting until after the term startup event?)
- Security risk
- Impact on production services and customers
- Complexity of the proposed change
  - Who has reviewed the plan and any new or modified code?
  - How was the change tested?
- Ease of back-out

Current membership of the SLT Exception Committee and approval requirements are available on the Change Management page of the HUIT website at http://huit.harvard.edu/itsm.

4.5.1.3. Additional Requirements
During all term startups, in the event that a change is unsuccessful or results in an unplanned service interruption, the following requirements are in addition to the normal Change Management process guidelines:

- The change assignee will inform the Change Manager via email (changemanager@fas.harvard.edu) by start of next business day. The following information should be provided:
  - Change request number
  - Details of problems encountered, as available
o Service impact
o Customer impact

• The Change Manager will inform the term startup committee as necessary via email distribution list
• The change assignee will update the Change Request ticket with available details by end of next business day

4.5.2. Heightened Sensitivity
During these time periods, caution should be exercised when scheduling changes that would impact services that are considered critical to the specific business event.

<table>
<thead>
<tr>
<th>Business Event</th>
<th>Event Duration</th>
<th>Event Start</th>
<th>Event End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading Period</td>
<td>~1 week</td>
<td>First day of reading period</td>
<td>Last day of reading period</td>
</tr>
<tr>
<td>Exam Period</td>
<td>~ 1 week</td>
<td>First day of exam period</td>
<td>Last day of exam period</td>
</tr>
<tr>
<td>Commencement</td>
<td>1 week</td>
<td>Monday before commencement</td>
<td>Sunday following commencement</td>
</tr>
</tbody>
</table>

Table 7 - Heightened Change Sensitivity Periods
5. Process Flow

Start the Change Management process as soon as the customer, business, project or IT management authorizes the planning of the change, which typically should be well in advance of the minimum lead-time.

In the next several pages, the process flows for the following types of changes are illustrated:

- Standard Changes
- Normal Changes – which are further categorized into Low, Medium and High Risk
- Emergency Changes
- Major Changes

The process flows use “swim-lane diagrams” to illustrate which role is responsible for the activity. These roles are described in more detail in the following section titled “Roles and Responsibilities”.

1. Standard Changes

1.1. All requests for new additions to the Standard Change Library (templates) are processed and approved through the Change Advisory Board.
1.2. The Change Requester secures business approval, as identified in the Standard Change Model.
1.3. The Change Requester submits the standard change request via the ServiceNow tool.
1.4. The change is built, tested and deployed as outlined in the Standard Change Model.
1.5. If the change is successful, the Change Implementer updates the CMDB (if necessary) and closes the Change Request ticket.
1.6. If the change is unsuccessful, the Change Implementer backs-out the change based on the plan associated with the Standard Change Model.
   1.6.1. During the post implementation review, the Change Manager and/or CAB determine if the Standard Change Model should be removed from the Standard Change Library.
   1.6.2. The Change Manager closes the Change Request ticket.

2. Normal Changes

2.1. The Change Requester secures business approval as appropriate.
2.2. The Change Requester submits the change request, identifying whether the change is Low, Medium or High risk based on the Risk Assessment.
2.3. The Service Owners identify whether an approver is required for LOW or MEDIUM risk changes for their services. Service Owners must approve all HIGH risk changes to their services.

2.4. LOW RISK CHANGES:

   2.4.1. For Low Risk changes, an approval request is routed to the appropriate Assignment Group Approver, who reviews, assesses and authorizes the change for further processing.
   2.4.2. If the services impacted by the change request have identified additional approvers for low risk changes, an approval request is routed to those approvers who review, assess and authorize the change.
   2.4.3. If all approvals are obtained, the change request is routed to the Change Implementer, who proceeds to build, test and deploy the change according to the approved schedule. If all approvals are not obtained, the request is routed back to the Change Requester with an explanation.
   2.4.4. The Change Implementer updates the Change Record after the change is deployed.
   2.4.5. If the change is successful the Change Implementer updates the CMDB as necessary and closes the Change Request ticket.
2.4.6. If the change is unsuccessful, the Change Implementer executes the back-out plan and conducts a post implementation review (PIR).

2.4.7. The Assignment Group Manager validates the PIR record and closes the change request ticket.

2.5. MEDIUM RISK CHANGES:

2.5.1. For Medium Risk changes, an approval request is routed to the appropriate Assignment Group Approver, who reviews, assesses and authorizes the change for further processing.

2.5.2. If the services impacted by the change request have identified additional approvers for medium risk changes, an approval request is routed to those approvers who review, assess and authorize the change.

2.5.3. If all prior approvals are obtained, CAB members must approve or deny the change via the ServiceNow tool online, (does NOT require a face-to-face CAB Meeting).

2.5.4. If one third of the CAB approves the change, it is routed to the Change Implementer for build and test. If the CAB (or any other approver) does not approve the change, the change request can be routed back to the Change Requester with an explanation, or escalated to the in-person CAB meeting for further discussion.

2.5.5. Upon approval, the Change Implementer build, tests and deploys the change per the approved schedule and updates the change record.

2.5.6. If the change is successful, the Change Implementer updates the CMDB if necessary or closes the change request ticket

2.5.6.1. The Assignment Group Manager validates the CMDB update (as necessary) and closes the change record.

2.5.7. If the change is unsuccessful, the Change Implementer executes the back-out plan based on the change record, and conducts a Post Implementation Review (PIR).

2.5.7.1. The Assignment Group Manager validates the PIR record and closes the change request ticket.

2.6. HIGH RISK CHANGES:

2.6.1. For High Risk changes, an approval request is routed to the appropriate Assignment Group Approver, who reviews, assesses and authorizes the change for further processing.

2.6.2. An approval request is routed to additional approvers for impacted services, who review, assess and authorize the change.

2.6.3. If all prior approvals are obtained, the change is presented for review and discussion during an in-person CAB meeting.

2.6.4. If the CAB approves the change, it is routed to the Change Implementer for build and test. If the CAB denies the request, the change request is routed back to the Change Requester with an explanation.

2.6.5. The Change Implementer deploys the change per the approved schedule and updates the change record.

2.6.6. If the change is successful, the Change Implementer updates the CMDB as necessary.

2.6.6.1. The Assignment Group Manager validates the CMDB update.

2.6.7. If the change is unsuccessful, the Change Implementer executes the back-out plan based on the change record, and conducts a Post Implementation Review (PIR).
2.6.7.1. PIR is routed to the Change Manager for approval

2.6.8. The Change Manager validates the PIR updates and closes the change record.

3. Emergency Changes

3.1. The Change Requester determines that an Emergency Change is required (i.e., change needed to fix Incident).

3.2. The Change Requester immediately contacts the ECAB via the Change Manager and requests approval.

3.3. If the ECAB does not approve the change request, the Change Requester shall follow the normal change process.

3.4. If the ECAB approves the request, it is routed to the Change Implementer who proceeds immediately to build and (if possible) test the change.

3.5. If the change is successful, the Change Implementer creates or updates the change record and updates the CMDB.

3.6. The Change Manager validates the CMDB updates, informs the CAB at the next CAB Meeting and closes the change record.

3.7. If the change is unsuccessful, the Change Implementer executes the back-out plan and conducts a post implementation review.

3.7.1.1. PIR is routed to Assignment Group Approver for approval

3.8. After the PIR, the Change Implementer creates or updates the change record and the CMDB.

3.9. The Change Manager validates the CMDB updates, informs the CAB at the next CAB Meeting and closes the change record.

4. Major Changes

4.1. A project team or member of IT Management identifies the need for a Major change, creates a Change Proposal and sends to the Change Advisory Board via a ServiceNow change request.

4.2. The CAB assists with identification of impact, conflicts and stakeholders and requests and receives feedback from stakeholders and impacted parties.

4.3. The change record is routed back to the Change Requester with the CAB comments for impact analysis and communications needs.

4.4. The change proposal is presented to or reviewed by the Senior Leadership team and either approved or not approved.

4.5. If approved, change requests associated with the Change Proposal follow the change management process for High risk changes.
5.1. Standard Changes

Figure 1 – Standard Change Process Flow
5.1. Normal Changes

Figure 2 - Normal Change Process Flow, page 1
Figure 3 – Normal Change Process Flow, page 2
5.2. Emergency Changes

Figure 4 – Emergency Change Process Flow
5.3. Major Changes

Figure 5 - Major Changes
6. Roles & Responsibilities

6.1. Change Requester
The Change Requester is the person submitting and owning the Change Request. The Change Requester is usually an IT staff member. Their responsibilities include:
1. Secures appropriate business approval for the Change prior to starting the Change Management Process
2. Completes the ServiceNow Change Request ticket, in collaboration with the Change Implementer (see below)
3. Communicates status of the change back to the business or project team as necessary

6.2. Implementer/Assignee
The Change Implementer/Assignee implements and monitors the change (Requester and Implementer can be same person). The implementer’s responsibilities include:
1. Assist the Change Requester with change request ticket documentation as necessary
2. Build and test the change
3. Create the implementation plan, test plan and back-out plan
4. Upon approval, deploy the change during the time scheduled
5. Execute the back out plan if required

6.3. Assignment Group Approver
The manager (or designee) of the functional group implementing the change. Directors or managers of all process participant groups will designate one or more approvers for each group. The responsibilities of the Assignment Group Approver are:
1. Review and approve or advise on change requests submitted to their group
2. Coordinate the resources that implement the change (within their team as well as resources that may be outside their team)
3. Complete the Post Implementation Review (PIR) as necessary for unsuccessful changes

6.4. Change Approver for Impacted Services
Each Service and Offering Owner needs to identify whether an approver is required for LOW or MEDIUM risk changes for their services. Service Owners must approve all HIGH risk changes to their services. The designated approver(s) for a service or service offering are responsible for reviewing and approving or advising on change requests that impact their services.

6.5. CAB Member
Change Advisory Board (CAB) participants are responsible for reviewing and recommending actions regarding medium- and high-risk Normal changes, all Major changes, and any proposed Change Management process improvement. Please refer to “CAB Membership and CAB Meetings” section for expectations and responsibilities.

6.6. Change Manager
The Change Manager is responsible for functional implementation and operation of the Change Management Process and its activities. The Change Manager’s responsibilities include:
1. Validate the type and risk of the Change
2. Escalate approval delay issues
3. Chair the CAB meeting
4. Ensure post-implementation reviews are conducted per the policy
5. Ensure CMDB updates are completed
6. If an unauthorized change is discovered, escalate to IT Management
7. Report on Change Management activities
8. Educate IT staff on the Change Management process
6.7. Process Owner

The Process Owner is accountable for the success and strategic development of the Change Management Process.
7. CAB Membership & CAB Meetings

7.1. CAB Membership
The Change Advisory Board (CAB) is used for assessing Medium- and High-Risk Normal changes, Major Changes, and pre-authorizing the use of Standard Changes Models.

The Change Advisory Board (CAB) is the keystone of the Change Management process. Its primary purpose is to mitigate risk to the Harvard community, the IT environment, and HUIT by evaluating change requests from the perspective of business and end-user impact.

The CAB process, including documentation as well as discussion and feedback, also enables representatives from HUIT’s service areas to provide technical validation and consultation as necessary to reduce the risk of unplanned service interruptions.

7.1.1. HUIT CAB Makeup
The CAB includes permanent representation from all HUIT teams responsible for providing and supporting HUIT services. The success of the CAB (and to a large degree, the entire Change Management process) is dependent on the contributions of its members who represent these teams.

The director or manager of each participant team should identify a primary CAB member, with one or more alternates. Regular CAB meeting attendance should generally be restricted to this primary CAB member, with other team members attending as necessary to speak to, or on behalf of, specific change requests. This facilitates efficient discussion and decision-making while ensuring a voice for all groups across the organization.

7.1.2. Functions
- Regularly scheduled weekly meetings
- Review and approval of all significant changes and other changes as necessary
- Assist with comprehensive service impact analysis
- Conduct Post Implementation Reviews (PIRs)
- Ensure complete and accurate documentation of change requests
- Important: The CAB is neither a forum nor a substitute for project planning and resource coordination.

7.1.3. Member Expectations
- Attend a Change Management training class
- Commit to attendance (or have a designated alternate attend in your place)
- Actively participate in CAB discussion
- Have a solid understanding of the services your team provides
- Be empowered to make decisions on behalf of your team
- Communicate to your team relevant information about change and process discussion from CAB meetings
- Act as a Change Management advocate and resource within your team

7.2. CAB Meetings
Appropriate preparation is essential to ensure effective and efficient CAB meetings. To that end, all Change Management process participants should be familiar with these guidelines.
• Requesters should submit change requests on time and CAB members should review all pending changes prior to the meeting.
• All necessary testing and implementation resources should be secured prior to CAB review.
• When requesting approval to make a change, be prepared to answer the following questions, preferably in advance via a well-documented Change Request ticket:
  o From the end-user perspective, will there be a service interruption during the change window?
    ▪ If so, how long (and to what degree) will service be interrupted?
  o From the end-user perspective, will the appearance or usage of the service change?
  o What is the technical risk assessment and, if the same change has been made in the past, the success rate?
  o Is this an ideal date and time to implement the change, taking into account its urgency, its risk, and its impact on service availability?
    ▪ Utilization statistics are particularly valuable to inform this discussion.
  o What are the details of any testing that has been completed, and what testing will occur after the change implementation?
  o What are the details of the back-out plan, and who will determine whether or not to roll back the change if it is unsuccessful?
  o What communications (both internal and external) are necessary?
  o What internal and external documentation is necessary?
  o What is the expected support impact of the change and what steps have been taken to prepare the support staff?
  o Is the change dependent on other changes or does it conflict with other changes?
• When completing a PIR (post implementation review) regarding your change, please be prepared to help answer the following questions:
  o What aspects of the change were successful?
  o What specific aspects of the change did not go as expected, and why?
  o What was the end-user impact?
  o What are the action items that require follow-up?
  o What are the lessons learned for future improvement?
• As a CAB member, actively contribute (as described above), with a focus on suggestions to support improved outcomes.

7.3. Emergency CAB (ECAB)
A sub-component of the CAB, the purpose of the ECAB is to facilitate Change Request approval when a change must occur before the next scheduled CAB meeting. As documented in the Change Assessment section, the ECAB is responsible for business approval of Emergency changes.

A meeting of the ECAB is initiated by the Change Manager, and typically will be accomplished via conference call or email. Participants should include the Change Manager, the director of the group that owns the affected service, the individual responsible for implementing the change, the Incident Manager, and other CAB members as appropriate.
8. Change Management Policies

1. A single Change Management process is adhered to by all HUIT groups.
2. All Changes are logged, tracked, and managed in a single service management system (ServiceNow) from initiation through closure.
3. Only Changes approved according to defined process requirements and procedures are implemented.
4. Where possible, Changes should be scheduled into an established Maintenance Window.
5. Procedures are defined for the expedited approval and implementation of Emergency changes in response to Major Incidents, regulatory compliance, or security issues.
6. Assessment, evaluation and approval of all Changes will include:
   - An objective assessment of potential business impact and risk
   - Documentation of any anticipated service interruptions
   - Meaningful documentation of communication needs, implementation and rollback plans, and testing requirements and results
7. Post implementation reviews are conducted for
   - All Major Changes and Emergency Changes
   - Changes that resulted in Major Incidents
   - Or at discretion of the Change Manager
8. Incidents caused by a Change must be linked to the appropriate Change Record.
9. Standard changes are added to the standard change library upon approval by the CAB
10. The purpose of the Change Advisory Board (CAB) is to mitigate risk by evaluating change requests from business, customer and end-user perspectives.
9. Required Change Request Documentation

All Change Requests require a detailed accounting of all services impacted or potentially impacted by the change implementation, and the degree to which their functionality will be affected or interrupted. Include any change or impact to the user experience.

### 9.1. Communications Plan

All Change Requests require that communications be addressed. At a minimum, the following questions need to be answered by the communications plan for each Change Request, unless no communications are necessary:

- Who is the target audience?
- What is the message?
- What is the notification method?
- When will notification(s) be sent?

### 9.2. Back-out Plan

All Change Requests require that back-out measures be addressed. A plan summary should be included in the Change Request ticket.

Back-out plans should seek to minimize organizational impact of a failed Change. When possible, it is beneficial to predefine a “trigger” condition that initiates the back-out plan, or identify a specific point in the implementation timeline at which a back-out decision is made. In circumstances in which no back-out plan is feasible, every effort should be made to mitigate the potential risk of organizational impact if the change is unsuccessful.

The primary accountability for defining and, if necessary, engaging a back-out plan resides with the requester or implementer of an individual Change Request, or of the project with which the Change Request is associated.

### 9.3. Testing Plan

All Change Requests require that testing be addressed. Change Management is responsible for confirming that a test plan, where feasible, exists.

As a rule, testing should be conducted whenever possible; it may include functional, QA, and user acceptance testing, or other testing as appropriate. Additionally, testing should be conducted as possible after a change has taken place as part of a typical implementation plan to ensure that impacted services are fully functional.

Ideally, the following information should be included in the Change Request ticket:

- Staff member(s) responsible for testing
- Dates during which testing occurred
- Details of testing environment, as appropriate
- Outcome of testing, with details as appropriate

### 9.4. Implementation Rating

Upon completion, all Changes receive an Implementation Rating that assesses the overall quality of the change implementation. The change is rated using the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rating:</th>
<th>Successful</th>
<th>Problems Encountered</th>
<th>Change Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback Unnecessary</td>
<td></td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>No Unplanned Service Interruption</td>
<td>True</td>
<td>Either is False</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
Table 8 - Implementation Rating

The Implementation Rating should be documented in the Change Request ticket, with additional information attached as necessary to provide details that explain the reason for the rating.
10. Changes to Critical Services

A “critical” service is one whose availability is vital to the success of University business and whose interruption – whether scheduled or unscheduled – would affect end users broadly. Examples of critical services include (but are not limited to) the Harvard network, major data centers, email, and PIN.

This sensitive nature of critical services warrants an additional degree of scrutiny, approval, and communication in order to mitigate the increased risk that changes to these services present. In addition to existing Change Management guidelines and requirements, the following expectations apply to all changes to critical services.

10.1. Scheduling
All changes to critical services must be scheduled outside business or prime usage hours, with exceptions made for emergency changes upon Managing Director approval.

10.2. Approval
Changes to critical services typically require approval by the Change Advisory Board (CAB), unless a change has been confirmed to have no noticeable impact on service availability.

During identified periods of heightened sensitivity, such as Term Startup change freeze, changes to critical services require exception approval from the Senior Leadership Team (SLT).

10.3. Communications

Changes Without Service Interruption: Standard web posting and targeted email as appropriate.

Changes With Service Interruption: In addition to standard web and email notification, additional information is supplied as available regarding service impact, workarounds, and recommendations. Minimum recommendation includes three external communications:

1) Notice: 4-7 business days in advance (except in the case of emergency changes)
2) Reminder: 6-24 hours in advance
3) Follow-Up: upon successful conclusion (or if unsuccessful, via the major incident notification process)

10.4. Test Plan
The Change Request ticket must include detailed test plans for both pre-implementation and post-implementation testing, including a list of participants and details of the test environments.

10.5. Back-out Plan
All back-out triggers and associated distinct “go / no-go” decision points during the implementation timeline must be explicitly documented, as well as identification of who is responsible for making back-out decisions.

11. Key Performance Indicators
HUIT will focus on a few select Key Performance Indicators (KPIs) to measure the success and efficiency of the Change Management process. As the Change Management process matures, the KPIs may change to focus on different areas that need improvement.

- Number of changes implemented by type, team
- Reduction in the number and percentage of emergency changes
- Reduction in the number of failed changes / increase change success rate
- Number / percentage of changes where approval exceeded the lead time
12. Process Integration

12.1. Service Asset & Configuration Management

Change Management will be integrated with the Service Asset & Configuration Management process and configuration database (CMDB) based on the following scope:

- All servers managed by HUIT Infrastructure, including:
  - Server provisioning
  - Changes to a defined attribute of any server CI
  - Server decommissioning