Service Management Program

Change Management Process

March 30, 2017
Scope

The change management process applies to all Penn State Service Management participants, contracted vendors, and organizations that introduce or implement changes to the Penn State University technical environment. It ensures technological changes occur in a uniform and predictable manner. This document is used in conjunction with the change management policy document and all IT and security policies located at guru.psu.edu.

The scope of the Penn State Service Management Program change management process includes managing the:

- introduction of business applications and infrastructure components to the Penn State University technical environment; and
- modification of existing business applications and infrastructure components of the Penn State University technical environment.
Process

210.1 Change Classifications

A. Standard changes follow a streamlined and preapproved workflow.
B. Normal changes follow the standard workflow.
C. Emergency changes resolve a service outage, imminent service outage, severe service degradation, security issue, or regulatory incident.

210.2 Standard Changes

A. A requester can only select from available standard changes. A requester should only use standard changes from his or her unit and department.
B. Standard changes occur frequently and are reviewed by the unit change advisory board (CAB).
C. Standard changes with a failure rate of 10% or higher must be marked inactive pending a review by the unit CAB.
D. Standard change proposals must include records of three successful normal changes.
E. Change process managers maintain the standard change library. Each process manager is responsible for the health of his or her unit’s standard changes.

210.3 Normal Changes

A. Normal changes follow specific workflows that are determined by a risk evaluation.
   i. Low- and medium-risk changes follow basic approval paths.
   ii. High-risk workflow includes additional approvals by the unit CAB.
B. Changes that are marked successful with issues or unsuccessful require a post-implementation review (PIR). See Appendix A for information about PIRs.
C. A change that results in a high-priority incident requires a PIR.
D. A summary of the PIR must be attached to the change record or supplied in the Closure Notes field.
E. Changes that require modification after the approval step must be cancelled and resubmitted for approval.

210.4 Emergency Changes

A. Only emergency changes may be created after the change is implemented.
B. All emergency changes require a PIR.
C. A summary of the PIR must be attached to the change record or supplied in the Closure Note field.

210.5 Approval Groups

A. Approval Groups
   i. Approval groups are required for end-to-end services in the Penn State technical environment.
ii. Approval groups are not required for third-party or cloud-based services, but can be requested for such services.

B. Approval Group Membership
i. Approval groups require one assignment group manager and at least three assignment group members.
ii. The approval group manager should be the service manager so service managers are aware of all changes occurring to the services they are responsible for.
iii. The approval group manager cannot be a group member.

210.6 Approval Matrix

A. Standard Change Approvals
i. The unit CAB follows CAB approval rules to review and approve standard change proposals. The unit change manager will mark the approval on behalf of the CAB.

B. Normal Change Approvals
i. Low Risk
   a. Requires approval by the approval group manager and at least one approval from the approval group membership.
   b. Fails if the approval group manager or one approval group member rejects the change.
ii. Medium Risk
   a. Requires approval by the approval group manager and at least one approval from the approval group membership.
   b. Fails if the approval group manager or one approval group member rejects the change.
iii. High Risk
   a. Requires approval by the approval group manager, at least one of the approval group members, and a unanimous vote from the unit CAB.
   b. Fails if either the approval group manager, one approval group member, or the unit CAB rejects the change.

C. Emergency Change Approvals
i. Require approval from the approval group manager and one approval from the ECAB.

D. Change Advisory Board Approvals
i. Only changes on the agenda of the regularly scheduled CAB meeting can be considered.
ii. All CAB members at the meeting must submit a vote on each change.
iii. All CAB members at the meeting must vote in favor of a change for it to be approved.

210.7 Change Advisory Board (CAB)

A. The unit change manager facilitates the CAB. The unit change manager is responsible for:
i. Setting CAB agendas
ii. Submitting CAB approvals
iii. Balanced unit representation within the CAB membership
iv. Unit representation within the ECAB membership
B. The unit process manager verifies that the CAB or ECAB has the appropriate cross-functional representation.
C. CAB or ECAB members can suggest to the unit process manager other individuals who may be asked to attend a CAB or ECAB meeting to provide supporting information.

210.8  Emergency Change Advisory Board (ECAB)

A. The ECAB is a smaller version of the CAB that represents the major stakeholders who can be contacted at any time of day to approve emergency changes to the University's technical environment.
B. The unit change manager facilitates the ECAB.

210.9  Statuses and Codes

A. New
   i. Status where a record can be created and edited while the rest of the information is being gathered.
   ii. All plans and planned start and end dates are required before a change request can move to the assess status.
B. Assess
   i. Status where the change is given a risk assessment.
   ii. Risk assessments are unique to each change category.
C. Authorize
   i. Status where all approvals are made.
D. Scheduled
   i. Status a change record enters after it is approved.
   ii. The change record appears on the change calendar at this status.
E. Implement
   i. Status a change record enters after it is completed.
   ii. This status requires an implementation code and notes.
F. Review
   i. Status where a record is under a PIR.
G. Closed
   i. Status where the change manager has closed the change record.
   ii. If a change was implemented successfully, it will automatically move to this status three days after implementation.
   iii. A record in this status cannot be modified or reopened.
H. Cancelled
   i. Records that are not approved move to this status.
ii. Records that are past the approval status but require a scope change or modification move to this status.

210.10 Risk Assessment and Calculation

A. All changes require completion of a risk assessment at the assess status. Risk assessments consist of multiple predetermined questions that enable calculation of the risk of the requested change.

210.11 Linking Records

A. Incidents caused by a change must be linked to the appropriate change record.
B. Incident, request, or problem records that will be resolved, fulfilled, or fixed by a change must be linked to the change record.

210.12 Key Performance Indicators

A. Focus will be on the following key performance indicators (KPIs) to measure the success and efficiency of the process. Each KPI has additional data breakdowns:
   i. Number of changes implemented
   ii. Number of emergency changes implemented
   iii. Number of unsuccessful changes
   iv. Number of incidents caused by changes
   v. Number of changes where approval exceeds the lead time
   vi. Number of changes created after implementation (standard and normal only)

Special Situations and Exceptions

Any request for an exception to this policy must be submitted in writing and will be reviewed on a case-by-case basis. Exceptions may be permitted only after documented approval from the change process owner and process managers.

Process Compliance and Monitoring

The change management process manager will periodically audit change requests for policy compliance. The process manager will notify the appropriate executive manager of any policy violations.
Definitions

**CAB** – Change Advisory Board. Each participating unit has a CAB to review high-risk changes to services that unit provides.

**ECAB** – Emergency Change Advisory Board. Each participating unit has an ECAB to review emergency changes to services that unit provides.

Supporting Documentation

- Change management policy documentation
- Change management procedure documentation
- Penn State Service Management Program policy documentation
Appendix A: Post-Implementation Review Outline

Step 1: Setting the stage.
Purpose: To identify if we followed the documented process and to identify what can be done to improve data, documentation, plans, or process.

Ground rules:
- Criticism of process is OK.
- Criticism of people is NOT OK.
- This is an opportunity to get better; a learning experience.
- Feel free to point out what people did well.

Step 2: Origin
- Did this start as a request or story?
- Was this request made to meet compliance?
- What was the purpose of this request?
- Was it approved? By whom?

Step 3: Software Development Lifecycle (SDLC)
- Was the change developed in dev?
- Was the change imported into acceptance?
- Was the change tested by DevOps in acceptance?
- Was the change tested by a subject matter expert in acceptance?
- Was the change imported into production?
- Was the change made during the maintenance window?
- Was the change tested by DevOps in production?
- Was the change tested by subject matter expert in production?
- Was anything unusual about this change that precluded the normal testing?

Step 4: Did we follow change management?
- Was a change made?
- Did we fill out all the change record criteria?
- Was the quantity or quality of the record data enough to enact the change?
- Was the purpose and expected result clear in the change?
- Were there acceptance criteria?

Step 5: How was it resolved?
- How long did it take to realize there was an error after the change?
- How long did the back-out plan take to implement?
- Were any additional issues created by the back-out plan?
- What steps were taken to establish a workaround?
- How many incidents were generated because of this?
- Are there any remaining open incidents or problem tickets that need to be addressed?

We will provide a summary based on this conversation to the unit director, service owner, unit change manager, and the PIR group.

We will be transparent about any mitigations as a result of this PIR.
Appendix B: Change Advisory Board

What is a CAB?

A Change Advisory Board, or CAB, is a group of people tasked with evaluating changes to the IT environment. A CAB can be as simple as an email distribution list or as formal as a board that follows formal meeting procedures and is led by a chairperson. The culture and the business needs of the organization determine what type of CAB is appropriate.

The CAB comprises technical staff and key decision makers. There are no established rules for who is on a CAB. The change manager ensures the CAB contains the right people with the right information, knowledge, and background to effectively review each change.

It is common for a CAB to call in subject matter experts to help review and advise on specific change requests because of the nature of the change (e.g., a senior network engineer may be consulted for a requested change to a router).

CABs and change management are not the same. A CAB reviews change requests for risk and unintended consequences and advises the change manager of the CAB’s findings and recommendations. Change management is the broader capability that manages the entire process of requesting, reviewing, evaluating, approving, tracking, and overseeing all changes.

What is the composition of a typical CAB?

A CAB should be staffed with representatives from functional areas and technical disciplines and key decision makers and business stakeholders as appropriate. The change manager organizes and runs the CAB meetings.

Typical CAB members include:

- Senior network engineer
- Senior application development engineer
- Operations manager
- Service desk staff
- Server infrastructure engineer
- Senior security engineer
- Information security officer
- Business relationship manager(s)
- Service owners
- Business users
What does a CAB do?

The CAB is often misunderstood to be the change approval or authorization board. However, the CAB is merely advisory. Its job is to review proposed changes and advise the change manager of the results of its findings. The change manager is ultimately responsible for approving (or rejecting) changes.

A CAB should:

- Review Changes (CHG records). Use knowledge, experience, and background to assess changes for risks and unintended consequences
- Ask probing questions to fully understand the proposed change
- Evaluate the proposed change for risks and mitigation
- Ensure that business outcomes are documented and well understood
- Schedule and prioritize changes
- Evaluate if the proposed change will give the intended outcomes without adversely impacting the business
- Ensure the proposed time is appropriate (doesn’t conflict with business needs, other changes, or operational activities)
- Ensure technical and architectural standards are met
- Determine likelihood of unintended impacts
- Make recommendations to reduce risk, increase likelihood of success, and minimize business impact.
- May request a more in-depth, formal change evaluation for a given change.

CAB Meetings

The change manager always acts as the chair of any CAB meeting, either virtual or in person. The change manager should call CAB meetings at appropriate times to ensure the prompt and efficient handling of all changes. During high levels of change this could potentially be daily. A formal CAB meeting is necessary for complex, high-risk, or high-impact changes, or when major projects are due to deliver products. CAB meetings can be used to provide a formal review and evaluation of current changes, review of outstanding changes, and to discuss any impending major changes. In-person meetings should have a standard agenda.

The change manager should circulate a CAB agenda to allow CAB members to conduct impact and resource assessments before the CAB meeting. The CAB meeting the change manager organizes should consist of attendees who are relevant to the changes the CAB will consider. This includes attendees from other groups and parts of the business outside IT. Appropriate representatives must evaluate each change the CAB considers.
Sample CAB Agenda

- A review of all failed changes
- A review of all backed-out changes
- A list of changes CAB members must assess
- A review of all changes implemented since the last CAB meeting
- Change management successes for the period under discussion, i.e., a review of the business benefits seen as a result of the change management process (as appropriate)
- CAB considerations for each change (before authorization)
- Assessment of risk or impact on the business
- Effect on the infrastructure and customer service, as defined in the SLA, and on capacity and performance, reliability and resilience, contingency plans, and security
- Impact on other services that run on the same infrastructure or on software development projects
- Resource assessment—the IT, business, and other resources required to implement the change and cover the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required
- The impact on non-IT infrastructure within the organization
- Effect, risk, or impact of not implementing the change
- Other changes being implemented at the same time as the change being considered
- Technical capability and technical approval
- Financial approval (if required)
- Third party or supplier involvement in the implementation of the change
- Business approval (if required)
- Review or assessment of the change priority

CAB comments and issues

The change manager must document in the CAB meeting’s minutes all CAB comments on each change and any issues that the CAB discussed.

CAB recommendations and decisions

The change manager must document in the CAB meeting’s minutes all CAB recommendations and decisions the CAB discussed.
Version Control

This section provides document control in alignment with best practices and standards.

<table>
<thead>
<tr>
<th>Document number:</th>
<th>210</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document title:</td>
<td>Change Management Process</td>
</tr>
<tr>
<td>Document owner role:</td>
<td>Change Management Process Owner</td>
</tr>
<tr>
<td>Document owner name:</td>
<td>Refer to the Service Management Office (SMO) website, smo.psu.edu, for a current listing of process owner information.</td>
</tr>
<tr>
<td>Document location:</td>
<td>SMO website, smo.psu.edu.</td>
</tr>
</tbody>
</table>

**Revisions**

**Document revision**: Cover page must match last date and revision. Contributors and approvers cannot be the same. Approval of controlled quality documentation will be completed using the change management process by submitting a change request.

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Contributors</th>
<th>Approvers</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/18/2014</td>
<td>1.0</td>
<td>Converged document for ITX program implementation</td>
<td>Change Management Process contributors, ITX Program Team</td>
<td>Shared ITX Steering Committee, Draft Contributors</td>
</tr>
<tr>
<td>8/8/2014</td>
<td>1.1</td>
<td>Operational document review</td>
<td>Document reviewers</td>
<td>Operational review team</td>
</tr>
<tr>
<td>9/24/2014</td>
<td>1.2</td>
<td>Operational document review</td>
<td>Document reviewers</td>
<td>Operational review team</td>
</tr>
<tr>
<td>11/6/2014</td>
<td>2.0</td>
<td>Added shared procedures and miscellaneous ODR changes</td>
<td>Document reviewers</td>
<td>Operational review team</td>
</tr>
<tr>
<td>7/22/2015</td>
<td>2.1</td>
<td>Aligned policy with ServiceNow implementation and updated language for consistency</td>
<td>Change process improvement team</td>
<td>Process owner, process managers</td>
</tr>
<tr>
<td>1/11/2016</td>
<td></td>
<td>Updates for consistency with ServiceNow implementation and University branding</td>
<td>Change process improvement team</td>
<td>Process owner, process managers</td>
</tr>
<tr>
<td>1/12/2016</td>
<td></td>
<td>Update for consistency with ServiceNow implementation</td>
<td>Change process improvement team</td>
<td>Process owner, process managers</td>
</tr>
<tr>
<td>1/30/2017</td>
<td></td>
<td>Split document into separate policy, process, and procedure documents. Revised to reflect new change process.</td>
<td>Change process improvement team</td>
<td>Process owner, process managers</td>
</tr>
<tr>
<td>3/30/2017</td>
<td></td>
<td>Revised for consistency with current process</td>
<td>Change process improvement team</td>
<td>Mike Lenhart</td>
</tr>
</tbody>
</table>
This publication is available in alternative media on request.

The Pennsylvania State University is committed to the policy that all persons shall have equal access to programs, facilities, admission, and employment without regard to personal characteristics not related to ability, performance, or qualifications as determined by University policy or by state or federal authorities. It is the policy of the University to maintain an academic and work environment free of discrimination, including harassment.

The Pennsylvania State University prohibits discrimination and harassment against any person because of age, ancestry, color, disability or handicap, national origin, race, religious creed, sex, sexual orientation, gender identity, or veteran status and retaliation due to the reporting of discrimination or harassment. Discrimination, harassment, or retaliation against faculty, staff, or students will not be tolerated at The Pennsylvania State University.

Direct all inquiries regarding the nondiscrimination policy to the Affirmative Action Director, The Pennsylvania State University, 328 Boucke Building, University Park, PA 16802-5901; Tel 814-863-0471/TTY.