BUSINESS
TECHNOLOGIES

Change Management Standards & Guidelines

Document Owner: Gabriel Calderon

Author: Kenneth Sandlian

Date: 6/20/2014

Last Modified: 6/14/19

Purpose:

This document constitutes the formal communication of the Business Technologies Division (BT) policy of Change Management as generally defined in the Information Technology Infrastructure Library.

The objective of change management is to minimize service downtime by ensuring that requests for changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled and consistent manner.

Scope:

This policy applies to changes to service delivery configuration items (CIs, see ITIL), and mass changes to service access CIs, within the sphere of responsibility of the BT Division. All BT Division personnel, contractors and external vendors are subject to this policy.

A service change is any addition, modification, or removal (temporary or permanent) of a BT Division service or service component and its associated documentation. The need for a service change arises both proactively and reactively for a variety of reasons:

- Proactively - seeking business benefits such as reducing costs, improving services, increasing the ease and effectiveness of support, developing a new service
- Reactively - a means of resolving errors and adapting to changing circumstances (for example software upgrades to retain vendor support)

Service delivery configuration items are those service components that bring the service to multiple customers. Examples of service delivery items are servers, applications, storage, databases, network switches, cabling between distribution and access layer network switches, and privileged user accounts.

Individual changes to service access configuration items are not subject to change management. Examples of these items are desktop and laptop PCs, telephones, ports on access layer switches to which no service delivery CIs are connected, and regular user accounts. However, mass changes to service access configuration items are subject to change management.

All changes to PCI configuration items require change management.

Business Technologies Policy:

All changes to service delivery Configuration Items must be requested, reviewed, and approved in accordance with processes defined in the BT Division Change Management Process Document.

Changes may only be made as scheduled within the Change Request and only after approval by authorized parties. There are three types of Change Requests and each has particular approval parties defined as follows:

- STANDARD – Approval is by the Implementer's functional area Change Coordinator and are Low Risk / Low Impact
- NORMAL – Approval for Low Risk / Low Impact NORMAL Change Requests is by the Implementer's functional area Change Coordinator. Approval for all other NORMAL Change Requests is by the Change Advisory Board (CAB)
- EMERGENCY – Approval is by the Change Advisory Board

There are circumstances when the Change Advisory Board is not readily available, and an EMERGENCY change is required to maintain or restore a critical service. In that circumstance, and where the risk incurred by the change is no more than moderate, the change can be implemented without prior approval. However, a Change Request must be created as soon as possible to document the change.

For changes that require Change Advisory Board approval, the Change Requestor, Implementer, or Change Coordinator should attend a CAB meeting in person or by conference call to discuss the Change Request.

Compliance Audits:

Staff found to not be in compliance may be subject to disciplinary action.

Referenced Policies, Processes, and Procedures:

Change Management Process

Approvals

Approver Name	Role	Signature and Date
Robert Kastelittz	Senior Vice President of Technologies – CIO	
Chris Larivee	Senior Director of Infrastructure and Operations	
Cheryl Monroe	Director of Infrastructure and Operations	
Eric Lapperre	IT Manager of Engineering	

BUSINESS TECHNOLOGIES

Change Management Standards & Guidelines

Document Owner: Ken Sandlian

Author: Susan Summers, Ken Sandlian, Jamie Kuttenkuler

Creation Date: 12/4/2014

Reviewed and/or Updated Date:8/21/2018

- Regularly scheduled Change Advisory Board (CAB) Meetings occur on Tuesday at 1:00pm. The following individuals must attend the CAB meeting:
    a. The Change Management Process Manager
    b. All members of the CAB
    c. Any individual who has submitted a Change Request to be discussed during the CAB meeting

- Members of the CAB and Change Coordinators are nominated by the Change Manager and Change Management Process Owner in coordination with the individual's supervisor. Here are the criteria for each role:
    - CAB Member
        - Must have broad technical experience and knowledge of the business
        - Although not required of each member, the CAB must have some supervisor and/or management presence
        - Must have availability to attend CAB meetings and to quickly review any emergency Change Requests
        - Must have an interest in the Change Management process, investigating Change Requests, and working across Technologies to resolve conflicts
        - Preferably, the CAB is represented by most of Technologies operational and development teams.
        - ITSM recommends business customer presence on the CAB. Although the CAB is not usually represented by a business customer, we include business customers in the change approval process via the System Shutdown Request process
    - Change Coordinator
        - Must be a subject matter expert in their area
        - Preferred to be a senior technician or supervisor, someone who is considered as a mentor in their team
        - Must be fluent using the Change Management process within AskIT. Training can be provided
        - Must have good communication and collaboration skills
        - It is preferred that the individual has knowledge of the business
        - It is preferred that the individual is process and detail oriented
        - The Change Coordinators group must include two Change Coordinators per team

- Change Request (CR) Levels of Approval:
    - STANDARD (Type = Standard) CRs are approved by the Change Coordinator. The Change Coordinator is typically the Implementer's section Subject Matter Expert (SME) but may be within the Requestor's section or one of the Change Managers. The Change Coordinator asserts, by approval of the CR, that the change being performed meets all definitions of a STANDARD change request as stated in the Change Management Policy, Process, and Procedures documentation;

- Normal (Type=Normal) CRs with both Risk and Impact levels of Low are approved by the Change Coordinator. The Change Coordinator asserts, by approval of the CR, that the change being performed meets all definitions of a Low Risk / Low Impact change as stated in the Change Management Policy, Process, and Procedures documentation;
- Normal CRs with Risk and/or Impact above Low are approved by the CAB with approval recorded by a Change Manager;
- Emergency (Type=Emergency) CRs are approved by the CAB with approval recorded by a Change Manager;
- Changes rejected within the System Shutdown Request process override CAB approval of a CR;
- Neither the Change Requester nor Implementer may act as the Change Coordinator for the CR.

➢ The DIA Standard Maintenance Windows are: Tuesdays, Wednesdays and Thursdays 2300-0500:
- Changes that cause outages for critical services shall be scheduled during defined and approved Maintenance Windows;
- Changes that are certain or likely to result in a service outage, even within a Standard Maintenance Window, still require submission and approval of a System Shutdown Request and may require a User Notification;
- The Standard Maintenance Window can be superseded by a specific Service Level Agreement (SLA);
- Changes to major infrastructure components (particularly network) have priority during Standard Maintenance Windows.

➢ All CRs require at least a 24-hour wait period from the time the CR is submitted to the Scheduled Start date/time unless:
- The CR Type = Emergency;
- The CR Type = Standard and the CAB-approved SOP indicates that the change does not require the 24-hour wait period.

The wait period is necessary to allow the Change Coordinator and CAB time to review the request. Any CR that comes in with less than a 24-hour wait time will be reviewed during the following CAB meeting.

➢ Technologies System Shutdown Requests:
- Should be submitted at least 5 business days before the scheduled change;
- The System Shutdown Request must be approved by a member of the Airport Operations and Maintenance Control Center groups. The Baggage System is represented as an approver of Technologies System Shutdown Requests, but their approval is not required.

➢ STANDARD CRs must include a URL link to a CAB-approved SOP in the SOP Library.

➢ SOPs referenced in STANDARD CRs must have a roll-back plan included in the Procedure section.

- STANDARD CRs do not require a Change Plan or Backout Plan in the Planning section of the AskIT Change Request form (the referenced CAB-approved SOP should have both). All other types of changes do require this information.

- SOPs used for the *Change Management Process* require 2 approvals, the Process Owner & the CAB
  - Prior approval of the SOP by the Process Owner is required before the SOP is brought to the CAB for approval.
  - The Change Manager (or their delegate) will then record CAB approval or rejection of the SOP.

- All CRs with Risk or Impact above Low should clearly indicate what services and users are affected.

- CRs in AskIT can be CANCELLED at any time prior to completion of the Execute Task.

- The Change Manager may approve any request to reschedule the implementation of a change or require that the CR be cancelled and a new one created.

- The Change Review Task for Normal CRs with Risk or Impact above Low should be completed by the Change Coordinator before the regular scheduled CAB meeting.

- The Change Execute Task should be updated and closed with an appropriate status and comments within 24 hours of completion of the change.

- The Change Post Implementation Review (PIR) Task should be completed within five working days of close of the Execute Task.

- During a Major Incident, any scheduled Changes will be suspended.

    - The Change Manager or MOD will announce the suspension of change execution to Technologies staff.
    - Following the resolution of the Major Incident, there will be a waiting period before changes can be implemented. The duration of the waiting period depends on the type of Major Incident.
    - The Change Manager will announce when changes can be executed following the Major Incident.
        - This requires the Change Manager to be in agreement the MOD or Incident Commander.
        - Also requires verification that the environment is stable from technical subject matter experts.

- Any changes made to the environment to support the resolution of the Major Incident should be recorded and tracked as Change Records in AskIT within four (4) calendar hours of the resolution of the Major Incident.
  - The Incident Recorder is responsible for this.
  - All Change Records created as a part of the Major Incident must be linked to the Incident record in AskIT.