**Digital River**

**Change Management - IT Change Control Information**

**What is Change Management?**

**Change Management is in the process of restructuring the CAB and its related processes. Some of the information on this page may not be relevant at this time.**

If you have any questions, please email them to the Change Management distribution list.

Thank you for your patience during this period as we update this process.

Change control documentation and communications may be reviewed by the Change Manager and/or CAB and will be audited for IT Certification (compliance to IT Change Control Policy.)

The Change Control Policy applies to all production IT changes and is to be used as a guideline for non-production changes. All production environment changes need to have a Change Control created in the ITSM tool using the Change Control functionality.

**CAB :**

The Change Advisory Board (CAB) is charged with ensuring proposed changes are viable and will not adversely impact the delivery of production services.

The CAB also oversees ITIL V3 and CMMI level 3 compliance. See Overview and Charter(save as .docx) for more details.

***CAB Meetings are held 9am central on Wednesdays in a Conference Room to be determined. New agenda items should be requested by preceding Friday.***

**The information on this page represents a high level view of the complete Change Management Process. All Change Management documentation can be found at the following link:**

**Change Control Documentation**

**ITIL framework for change management divides changes into three categories:**

**Normal Change:** A Normal Change is one for which an assessment and evaluation must be completed. The Change Manager will utilize the Change Advisory Board (CAB) as well as Senior Management to determine the best solution and approval.

**Release Management:** A Release Management Change is one that is related to a Software Release. The Change Manager will utilize the Change Advisory Board (CAB) as well as Senior Management to determine the best solution and approval

**Standard (Pre-Approved) Change:** A pre-approved Change that is low Risk, relatively common (i.e. done frequently) and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. Request for Change (RFC)'s are not required to implement a Standard Change, and they are logged and tracked using the ITSM Change Control functionality. All Standard Change executions must be implemented successfully at least once as a Normal Change previously CAB approved request.

**Emergency Change:** An Emergency Change is one that must be completed to restore service and is related to an active Tech Center P1 or P2 Major Incident.

**Normal Change Control**

**PRE Change**

A Change Control may be created in the ITSM tool Service Manager. If help is needed using the ITSM tool please email Change Management.

1. Provide all data and complete all of the phases to the Technical Approval phase

* Registration
* Build and Impact Analysis
* The Build and Impact Analysis phase requires the scheduled deployment date, Risk Assessment, Deployment Plan, Back Out Plan, Test Plan and Test Results. Once filled in and saved this change will appear on the Release Calendar and be reviewed by the CAB.

1. The Technical Approval phase requests Manager's or Director's approval
2. Please attend the CAB meeting to:

* Provide a high level overview or summary of the change
* Provide information on system/application impact
* Provide information on Client impact
* Provide worst case scenario
* Answer questions

***IMPORTANT NOTE: All Planned changes require all of the "PRE Change" phases to be completed by 8:00 pm CST Tuesday before the change is scheduled to be reviewed by CAB. If you need an exception to this rule, it will need to be approved by your Manager in the ITSM toolset.***

Note: To implement a Normal change using the defined gC Maintenance Window see Section 5 on the Change Advisory Board page: http://confluence.mpls.digitalriver.com/display/ITIL/Change+Advisory+Board.

**Change Communications**

* Normal Changes
  + Communicated during the weekly CAB meeting in advance of the change.
* Releases
  + Our communicated through the Release Calendar with an appropriate time window.

**POST Change**

1. Review the change control making sure all data is complete.
2. Close the change control by completing the "Closure" phase.

**Thoughts and suggestions on filling out the fields and text boxes in the Change Control:**

* Please use professional language.
* Please make sure all fields and text boxes are complete with change details
* The Title in the Change Control should begin with indication of community impacted by change, for example:
  + GC: v4 properties modification (JDO cache ttl)
  + DC1: Install disk tray dc1hitachi02
* What is the business case/need for the change?
* What is the change supposed to do?
* How are you going to make these changes?
* How are you going to QA your changes?
* What is the backout plan?
* What systems/platforms are affected by these changes?
* When are you planning on implementing these changes?
* Notification/Communication Plan?
* Managers can approve Change Control entered and being completed by their direct reports.
* Managers that request a Change Control need to have the change approved by the manager's supervisor or above.
* Do not implement the change until the Change Control has been approved and is in the Deployment phase.

**Standard Change Control**

***Standard Changes must be approved by Change Management and IT Leadership in order to be recognized as a regularly occurring, well formed change event that does not require the same documentation, approvals and lead time expected for changes in the Normal category. All change details must be documented in the ITSM Tool under the Change Management functionality.***

**Guidelines for Standard Changes**

* The change must be completed as a "Normal" change prior to the submission of the Standard Change request
  + This is to insure the steps and tasks outlined in the Standard Change request execute as desired
* If the execution of a Standard Change causes any issue
  + the standard change approval is revoked
  + the standard change will be disabled in the ITSM tool
  + future executions of the change must be completed as a "Normal" change until approved as a standard change
* All Standard Changes will be reviewed by requester, IT Leadership and Change Management as deemed necessary
  + DR is a very dynamic environment. A Standard Change today does not mean it is still applicable one, two years hence.
  + The review will look at execution frequency
  + Issues created
  + Current applicability
  + Current risk
  + Steps/tasks still current

**Process for Execution of an Approved Standard Change**

1. For each execution of an Approved Standard Change complete a change in the ITSM tool
2. Use the Category "Standard Change"
3. After the new change form is opened, select the correct template from the list displayed after pressing the "Apply Template" button
4. Fill out the change form
5. Implement the change
6. Close the change

**Emergency Change Control**

An Emergency Change Control is necessary to track changes that are made immediately due to a production issue, or in response to a severe, impending production issue. IT associates follow the Escalation Management Policy, if possible, and make the change in production. They log the change in the Digital River Service Manager application using the Change Management functionality. Communication of the change is via e-mail.

**PRE / DURING Change**

1. Notify a manager or director and ask for approval to move forward. Only in the case of a severe issue should you move forward without informing management. Managers can give approval verbally but must update the DRSM Emergency Change record when time is allowed.
2. Communication is very important during production incidents. Seek a consensus, ideally on a conference bridge from peers before making changes.
3. Add an entry in the Digital River Service Manager

* You should already be trained on the use of this tool. If not contact the Change Manager
* Implement the change.

**POST Change**

1. Complete the change control in Service Manager detailing the trouble shooting steps which were taken, the issue found and the change made.
2. Relate the Incident to the emergency change.
3. If necessary, follow up with the impacted application developers regarding the change.
4. Complete a Root Cause and Corrective Action (RCCA) analysis when it is provided to you

* Create and/or request that a Change Control be completed for any further action that needs to be taken to solve the root cause and keep the emergency from recurring.

**ESCALATION/Incident Management**

**Timeline for Escalating Production Incidents to Management**

Any issue impacting production platforms for 10 minutes or more must be escalated. In the event that you cannot reach one layer of management, proceed with the escalation to more senior management until someone is reached.

***Time 0: system issue found & Unix hotline called or other staff notified, Technical Center notified***

***T + 5-10 min: System Admin/Engineer on-call staff contacted (IT Phone List)***

***T + 15 min: Director/Manager responsible for the impacted system called***

***T + 20 min: Director/Manager responsible for the impacted system calls Group VP***

If assistance is required from a particular platform/department, notify the ***Technical Center*** to gain their involvement.

**Escalation Protocol:**

* File an Escalation, if one has not already been created
  + Contact Technical Center:
    - Phone: **888-898-1898**
    - Email: **TechnicalCenterTeam@digitalriver.com**
* The Technical Center will open a conference bridge and communicate out to necessary people.
* The designated conference bridge will be a central point of communication for any changes and decisions.
* Personnel from the IT or Dev teams, as appropriate, will be asked to lead the bridge.
* All changes must be communicated to the conference bridge and the leader.
* All decisions, changes and issues will be documented by the Technical Center, with the following details:
  + Start time
  + End time
  + Person making the change or discovering the issue
  + If an issue - document possible causes and stack rank by likelihood
* The Documenter will select a time zone to record notes in and communicate with.
* Only one change will be made at a time and verification (testing) of expected behavior will occur immediately following.
* Be transparent with your communication and issues you uncover. Do not hold back possible problems.
* Stack rank open issues.

**Roles needed filled on escalation Conference Bridge at ALL times:**

1. **Leader:**

* This person, a member of the IT or Dev teams, will ensure order on the bridge and communication
* All changes must be heard by the leader and agreed to before taking action
* Leader should ensure troubleshooting continues to progress in a timely manner.
* Leader will gain group consensus as needed.
* Leader should verify time of changes with documenter and staff making the changes.

1. **Documenter:**

* An Agent of the Technical Center, responsible for maintaining the record of all decisions, changes and issues in agreed upon time zone.
* The Documenter should not be actively participating in the troubleshooting/changes that are taking place.
* The Documenter should clarify actions, timeframes and owners.
* The bridge log should include detail about when relevant items/issues are discovered, when decisions are made, when changes are made, when changes are verified, etc...
* The Documenter will confirm with the Leader who is the RCCA owner for the escalation.

At the conclusion of the escalation the log should be saved and attached to the incident within the Incident Log.

1. **Communicator:**

* The Communicator will be an Agent of the Technical Center and may also be the Documenter.
* Responsible for communicating status out via email on at most a 30 minute or as needed basis to necessary people (e.g. Executives, Escalation Team, other defined teams, etc.)
* Responsible for contacting additional needed parties to join the escalation bridge.

1. **Hands-on staff:**

* Responsible for implementing approved changes and communicating details back to the bridge
* Must communicate start/end times and details of changes made to Documenter
* Responsible for communicating open issues to the Documenter and all on conference bridge

**POST Escalation Tasks:**

1. Complete a Root Cause and Corrective Action (RCCA) analysis.
2. Create Service Request tickets for any further actions that need to be taken to solve the root cause and keep escalation from recurring.
3. Fill out the RCCA document and return to the Technical Center within 48 hours.
4. Technical Center will review and document details from the RCCA within the Incident Log.