Change Management FAQs

Article ID: KB0013179
Created: 2021-12-02 13:24:40
Updated: 2021-12-02 13:25:13
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/c39a6bc26fb9860070404a950d3ee41e', 'value': 'c39a6bc26fb9860070404a950d3ee41e'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/fc7d1a0987177494e3f297d83cbb3570', 'value': 'fc7d1a0987177494e3f297d83cbb3570'}

Where is the full Change Process Document and Standard Operating Procedure (SOP)?

Fresenius DTI Change Management Process - version 4

Standard Operating Procedures

What is a DTI change?

The ITIL® definition of a change is the addition, modification or removal of anything that could have an effect on IT services. What should be considered a change and how do we treat it as to minimize impact and risks, while being certain to meet the real needs of our users? There is no change without risk, and this risk must be known and managed.

What are the types of production changes in the DTI Change Process?

Standard change

A standard change is one that is frequently implemented, has repeatable implementation steps, and has a proven history of success. It is generated from an approved template in the Standard Change Catalog and follow a streamlined process in which technical approval and CAB authorization steps are not required. This enables the Change Management team to control the changes that are authorized as standard.

Some examples of standard changes include Software patching and updates; Firewall changes; New DNS entries; or service/daemon restarts

Emergency change

A change that must be implemented as soon as possible so cannot wait for the normal lifecycle of a change. This change is a high priority, so it bypasses technical approval and goes straight to the Authorization state for approval by the eCAB approval group. The valid use cases for an emergency change are: During a Major Incident in order to restore service/functionality which has failed

To prevent imminent adverse impact to:

Patient CareSecurity OperationsFinancial ImpactRegulatory/Compliance

Examples of valid reasons for an emergency change:

A Major Incident is in progress to restore a clinical applications functionalityAn issue with the server firmware causes a potential security issueFinancials code must be corrected before a nightly job runs which would cause issues.

Examples of invalid reasons for an emergency change:

A deadline was missed for changeBusiness partners have requested a change be implemented sooner

Normal change

Any service change that is not a standard change or an emergency change.

Normal change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed. These changes require a full range of assessments and authorizations such as technical approval, formal risk assessment, and Change Advisory Board (CAB) authorization (for High or Moderate risk changes), to ensure completeness, accuracy, and the least possible disruption to service. These changes are most often scheduled outside of defined change blackout/freeze windows or during defined maintenance windows.

Are Data updates changes?

Updates to data, done in the normal daily operations of a system with standard application user interface governed by Security roles, does not constitute an ITIL Change, and does not require Change Control process.

Modification of data done outside the normal user interface that may have an impact on upstream or downstream applications does constitute an ITIL Change, requiring Change Control process.

Any changes to application configuration by an application administrator which effects an IT service, regardless of whether it is done via a standard user interface or not, does constitute an ITIL Change, requiring Change Control process.

Examples:

Chairside care givers that enter data into our clinical systems does not constitute a change and does not require DTI Change Control. Data updates being performed by a DTI group by running a SQL script or ad-hoc query, does require DTI Change Control.Bulk Medical Records updates, duplicate processing, or other bulk data updates does require DTI Change ControlChanging a configuration setting to the OnBase application using the Hyland administration tool requires Change Control. Updating Firewall rules requires Change Control.

Do Service Restoration activities require Change Control?

Service Restoration means the act of returning failed managed devices/applications/functionality to a usable state. Restoration does not always refer to the final fix action and may include interim solutions such as user workarounds. A temporary solution can remain in use until a Final Resolution for the request can be determined and implemented.

Any addition, modification, or removal of anything that could have an effect on DTI services requires change control. This may include standard and emergency change types.

Does a server reboot or a service/daemon restart require Change Control?

Note: to simplify reading, the term reboot also refers to restarting services or daemons.

Yes, a reboot is a change (can be a standard change). Why a change record needs to be logged for it? Logging a change record also provides a record of the work performed. These historical records can be invaluable to Problem Management to identify trends and perform root cause analysis if need be.

In case of an emergency, engage the Major Incident Manager so that he/she can start the communication that a reboot will be taking place, and log the change after the reboot took place. A reboot can be a standard change.

1. The reboot actually changes the status attribute of the Configuration Item. For example: It is changed from “Live” to “offline” and then again to “Live”. Although the result is identical to the original state, the status did change even though it may not have been recorded in the CMDB.

2. The ITIL® definition of a change states that it is “...anything that could have an effect on IT services.” Rebooting is somewhat of a severe impact to a service since for that moment in time the service is actually unavailable while the reboot is taking place (I.e. the service does not exist during this time). Thus, rebooting without reviewing the potential impact can cause additional incidents.

3. The purpose of Change Management is to ensure “that standardized methods and procedures are used for the prompt handling of all changes.” Part of these procedures is to communicate. Thus, service owners and application administrators can properly/gracefully shut down their application. They are also aware that they may need to restart them, manually restore interfaces, etc. Failure to review the impact of a reboot and to communicate can result in unnecessary down time and lost effort if a team is unaware of the reboot and is under the impression that they are dealing with an incident when the service goes offline.