Cheatography

Change Management Cheat Sheet

by Corliss Thornton (corlisspt) via cheatography.com/23307/cs/6716/

Change Management

• Controls the lifecycle of all changes
• Responsible for formal assessment of a new or changed IT service
• Ensure that risks have been managed
• Helps determine whether to authorize the change.
• Enables beneficial changes to be made with minimum disruption to IT services.

Change Request Requirements

• Impact statement/assessment
• Implementation Plan
• Tasks or milestones needed to implement change
• Back out plan
• Anticipated downtime start and end times
•Draft customer notification of anticipated downtime
• Communications plan w/draft communications*
• Test Plan, Test Case, and Test Summary Report*
• Other plans as needed (e.g. capacity, transition, and release and deployment plans)*

(*) These items aren't required for every change. However, if you are unsure if it is required for your change request please check with the Change Manager.

Characteristics of a Standard Change

Low in risk, impact and visibility
Relatively common
The tasks are well known, documented and proven
There is a defined Roll-Back plan
Testing may be required
RFC Submitted into SDP
Pre-authorized change - CAB approval not required
Report weekly to CM/CAB

Examples of a Standard Change

Any change that does not alter the specification of a Configuration Item (CI)
Testing of an application, service or development project that will be introduced as a part of normal change
**Some standard changes are not documented in the change management process; but instead are documented in incident management process using a ticket submitted to the Service Desk.
**However, a normal or emergency change may be triggered by a ticket in the incident management process
**Therefore, it is not a standard change just because it started as a ticket within the incident management process… you must evaluate each change or trigger individually

Note: This is not an all-inclusive list

Standard Change Requirements

• Notification of the implemented change to the Change Manager by the start of the weekly CAB meeting.
• A change request and/or incident report if determined that it should have been implemented as a Normal Change including communications and other documentation as relevant.
• Entry into the event schedule by the Change Manager.

Characteristics of a Standard Recurring Change

Reoccurs on a standard timeframe (weekly, bi-weekly, monthly, etc...)
Has same characteristics as a Standard Change but requires approval by the CAB
Report completed occurrences to CM/CAB
Low in risk, impact and visibility
Relatively common
The tasks are well known, documented and proven
There is a defined Roll-Back plan
Testing may be required
RFC Submitted into SDP

Examples of a Standard Recurring Change

Any change that does not alter the specification of a Configuration Item (CI)

Testing of an application, service or development project that will be introduced as a part of normal change

**It is possible for a recurring normal change that has been implemented successfully a couple of times to become a standard recurring change for future deployments.

Note: This is not an all-inclusive list

Standard Recurring Change Requirements

• Notification of the implemented change to the Change Manager by the start of the weekly CAB meeting.
• A change request and/or incident report if determined that it should have been implemented as a Normal Change including communications and other documentation as relevant.
• Entry into the event schedule by the Change Manager.

Types of Changes

Standard

Standard Recurring

Emergency

Normal

If a change is implemented outside one of these processes, it is an unauthorized change.

Note

Most changes should go through the normal or standard change process.

Emergency changes should not occur very often.

If a change is implemented outside one of these three processes (standard, normal, emergency), it is an unauthorized change.

Characteristics of an Emergency Change

Requires immediate attention

Usually in response to break/fix issue. They should never occur because of poor planning.

Restoring service, preventing an outage or repairing an error that is severely impacting business

Testing reduced or forgone

ECAB notified verbally or via email

RFC submitted w/in 1 business day of implementation or fix

ECAB approves

The percentage of Emergency changes occurring in the environment should be very low.

Examples of an Emergency Change

A location is without a service

There is a severe degradation of service needing immediate action

A system/application/component failure causing a negative impact on business operations

An enterprise application is unavailable

A response to a natural disaster

A response to an emergency business need

A security breach requiring a patch to an enterprise server, enterprise application or a large number of workstations

Hardware malfunction has required a SQL database to be restored to another server

Corrupt data from an interface requires the database to be restored from backup

Reboot of a domain controller in a network outage situation

Nola.gov website is down

Note: This is not an all-inclusive list

Emergency Change Requirements

• Submission of a Change Request within one business day after the issue has been resolved
• Post implementation review of the Emergency Change at the next CAB meeting
• May require submission of an incident report to the Change Manager and/or Security Administrator
• May require engagement of an incident response plan if the change request is the result of a hacker
• Communications may be needed

Characteristics of a Normal Change

Testing may be required

Not an emergency or standard change

RFC required w/ supporting documentation

CAB approves

Examples of a Normal Change

Change that results in business interruption during regular business hours

Changes in any system that affects disaster recovery or business continuity

Introduction or discontinuance of a service

Move new development projects into production

Create/update an image for a large number of computers

Apply/install an enterprise application upgrade, service pack, patch, hotfix, etc…

Apply/Install a server operating system patch, hotfix, service pack, etc…

Add, relocate or decommission a server

Implementing a new domain policy

Upgrading domain controller

Install or relocate a printer that is high impact for a mission critical function

Changes to active directory

Examples of a Normal Change (cont)

Hardware failure to be fixed by a vendor

Note: This is not an all-inclusive list

Normal Change Requirements

See section: Change Request Requirements
• Also requires approval by the CAB

Characteristics of an Unauthorized Change

Implemented without approval of Change Manager or CAB

Requires submission of incident report & RFC; maybe incident response plan

Reported to Change Mgr & Security Admin

CAB determines… Valid? Reversed? Privileges revoked? Disciplinary action?

Need more information?

If you need additional information or need in-depth information, read the "ITI Change Management Process" document or go through the Change Management Process training material.

By **Corliss Thornton** (corlisspt)
cheatography.com/corlisspt/

Published 22nd January, 2016.
Last updated 7th December, 2017.