

CD Business and Infrastructure Apps Change Risk Classification Guidance

This document provides guidance for determining the risk associated with a change. Within Change Management, the level of scrutiny of a change is a function of its risk.

1. Work

Day-to-day work is made up of very low risk activities. Day to day work is not tracked and entered into the Remedy Change Management System. Work can be performed at any time and is not restricted to normal maintenance windows. Changes governed by other policies (for example computer security incident response actions) are considered work.

Approval Required: **None**

Guidance: Changes to process and policy documents that are editorial in nature and do not materially affect work or decisions. Changes to data, which are considered normal operations of the system like entering/modifying data using pre-existing forms. Running existing scripts to update/add/delete data. Anything that requires a Harvest/CVS package is NOT considered work.

Examples

- Changing crontab entries
- Using any published interface to enter or alter data – e.g.:
 - adding bins to tape vault,
 - modifying userdb user information (e.g. employee badge type changes from V to N)
 - adding new admin assistant to leave admin,
 - adding new gatekeepers to MISER roles,
 - changing Budget Input using existing forms,
 - modifying data on maintenance contracts (using sqlplus),
 - generate one-of report
 - end of FY changes for purchasing
 - adding new persons in workflow roles
 - using the manual event injector functionality of TIssue to create new events
- Cosmetic changes to a report (fixing a misspelled word)
- Fixing Plone items when they are in a “fallout” state
- Recompiling Oracle packages that have become invalid
- Changes to documentation
- Putting on a hat and doing an approval for someone having problems with a requisition/leave request/etc...
- Forcing manual Miser req state changes

- Adding new database data types
- Granting access to database packages
- Restarting daemons, services, background processes, batch jobs ... Example – Oracle Application Server, apache web server, NIMI/Tissue daemons/services etc...
- Changes to application configuration files. E.g. Adding Oracle DAD's, apache htaccess, NIMI config

2. Standard Change (Risk Level 2)

Standard Changes are low risk, routine changes to the production system performed according to a template that has successfully navigated the Proposed Standard Change process at least once. Standard Changes must be moved to production during the group's standard maintenance window for moving changes into production.

Initial Approval Required:

Authorization to build	Group Leader or Line Manager
Approval to go live	Pre-approved

Final Approval Required:

Authorization to build	Pre-approved
Approval to go live	Pre-approved

Guidance: Changes to software of limited audience, function, and low engineering risk with little potential to embarrass the division/lab. The change shall not include any underlying database schema changes. Administrative actions limited to data and configurations for one application. Simple report changes like adding a column, changing the sort order etc. Simple online form changes like changing font size etc. Configuration changes that do not require downtimes in excess of 5 seconds.

Examples:

- Changes to an existing web displays of data
- Adding a new MISER document type
- Recompiling an ora_pkg_tools release to incorporate the latest Oracle interface
- Changes to the MMS batch and nightly sync. Jobs for CD/DO MISER.
- Adding new columns to existing database views and creating new views.
- Adding new web page read-only displays of data
- New report or changes to report output/format

3. Proposed Standard Change (Risk Level 3)

Proposed Standard Changes are standard changes going through the remedy change process for the first time or second time. Once a proposed standard change has successfully navigated this process, it will be approved as a standard change for future Requests for Change (RFC's).

Initial Approval Required:

Authorization to build	Group Leader or Line Manager
Approval to go live	Group Leader or Line Manager

Final Approval Required:

Authorization to build	Change Manager
Approval to go live	Change Manager

Guidance: See Standard Change Guidance.

Examples:

- See Standard Change Examples

4. Minor Change (Risk Level 4)

Minor Changes are non-routine, low risk changes to programs or applications that have limited impact. Domain-specific judgment shall be used to identify minor changes. Minor changes should pass the following risk screen:

- The staff reasonably expected to plan and implement a minor change have experience implementing equivalent changes.
- The change does not consume substantial people or technical resources, and those resources are expected to be available.
- There is high confidence that a back out plan can be developed and executed, if needed.
- The change is NOT directly responsive to an external requirement, such as a DOE requirement,
- The change does NOT significantly affect a large number of users, a large experiment, an important facility, or an important process or function of the laboratory. Changes completely supported by redundant and fault tolerant infrastructure of sufficient capacity need not be major.
- The change changes flow of money or tangible resources into or out of the laboratory at a level that does not exceed similar changes performed by the expected staff planning or implementing this change.

Minor Changes must be moved to production during the window that was approved by the Change Manager.

Initial Approval Required:

Authorization to build
Approval to go live

Group Leader or Line Manager
Group Leader or Line Manager

Final Approval Required:

Authorization to build
Approval to go live

Change Manager
Change Manager

Guidance: Bug fixes or enhancements to code to systems with limited audiences. New scripts that add/update/change data in a database Verbiage changes to process documentation, which are consistent with existing policy, and have a local impact on work practices. Dot releases (minor changes) to supported system.

Examples:

- New dot release of any existing package
 - Creating new scripts to process Kronos effort reporting data.
 - Tissue upgrade from version 1_0_10 to version 1_0_11.
 - CD/DO Miser enhancements(EPEAT gold/silver/bronze for example), bug fixes
- Creating a new network detector for Nimi

5. Major Change (Risk Level 5)

Major Changes are high-risk program, policy, or application changes that typically affect a large user base or a significant set of users. All changes, which are not Work, Standard, Minor, or Emergency, are Major. Domain-specific Judgment shall be used to identify major changes.

Major Changes must be moved to production during the window that was approved by the Change Manager.

Initial Approval Required:

Authorization to build	Group Leader or Line Manager
Approval to go live	Group Leader or Line Manager

Final Approval Required:

Authorization to build	Change Manager
Approval to go live	Change Manager

Guidance: Major upgrades to software packages, major configuration changes (environment or application specific). Changes to systems with a large audience.

Examples

- Tissue v2 – adding an event level exemption system.
- Miscomp changes to support Infoblocks.
- Rewriting existing applications with new technology e.g. changing Oracle forms to JavaScript or Crystal Reports.

Approved By: Michael Kaiser
Jim Fromm

Change Manager
Manager