

FERMILAB CHANGE RISK CLASSIFICATION GUIDANCE

Description	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.
Applicable to	High Performance Computing
Document Owner	<i>Change/Release Manager</i>
Effective Date	<i>04/28/2016</i>

VERSION HISTORY

Version	Date	Author(s)	Change Summary
1.0	<i>04/28/2016</i>	Michael Kaiser Amitoj G Singh	Initial document

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 Change Management System. Work can be performed at any time and is not restricted to normal maintenance windows. *Work should be tracked via a ServiceNow Incident Ticket or Requested Item Ticket. Alternatively work can be tracked via shared Twiki based documents which detail the plan, action, and back out process.* Changes governed by other policies (for example computer security incident response actions) are not governed by Change Management and are therefore considered work.

Approval Required: **None**

Guidance: Work includes changes to hardware/software documentation and other group documentation that is not controlled as part of a periodic audit review. Changes to data and system configuration, which come about through normal operations of the system or which are manual but affect only small parts of the data or system, are also categorized as work.

Examples:

- Adding new user accounts to the clusters
- Changes to existing disk quotas
- Diagnosing and solving batch queue issues
- Replacing and testing suspect disk drives
- Restoring service without changing the configuration (e.g. re-booting a machine or restarting part of the service, fixing monitoring)
- Sending damaged parts (power supplies, servers, drives, interconnect cards) out for recovery
- Troubleshooting Lattice QCD code failures
- Debugging incidents and problems in the production systems (this may include enabling detailed diagnostics for some period and restarting service components in some instances)
- Adding monitoring that will not affect production running

2. Standard Change

Standard Changes are low risk, routine changes to the production environment performed according to a template. Standard Changes must be moved to production during the group's standard maintenance window (if one exists).

Build Approvals Required:

- 1) Group Leader or Designated Alternate

Go Live Approvals Required:

- 1) Pre-Approved

Guidance: Changes to software/hardware with limited exposure, audience, function, and low engineering risk with little potential to embarrass the division/lab. Administrative actions limited to data and configurations for one application. Verbiage changes to process/service documents, which are consistent with existing policy, and have a local impact on work practices.

Examples:

- Annual review of ISO20K controlled service/process documentation.
- Replacing failed computers
- Adding new customers that have been approved at the department level
- Enabling Globus Online services, servers
- OS and supporting software infrastructure minor release patches and tuning
- Adding new file-systems into a production environment
- Infiniband Firmware updates
- Tested server/BIOS firmware updates. Application tuning changes that don't require a reboot or service restart and have low impact
- Diagnostic activities that involve code changes beyond increasing log levels
- Adding or removing Torque/Maui/PBS queues

3. **Minor Change**

Minor Changes are non-routine, low risk changes to programs, applications, systems, or equipment 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 does NOT alter the flow of money or tangible resources into or out of the laboratory at a level that exceeds similar changes performed by the staff planning or implementing this change

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

Build Approvals Required:

- 1) Group Leader or Designated Alternate

Go Live Approvals Required:

- 1) Group Leader or Designated Alternate
- 2) Change/Release Manager

Guidance: Fixes/enhancements to software/hardware affecting only one of the ITIL services/processes.

Examples:

- Minor hardware configuration changes.
- Significant kernel upgrades or OS configuration changes, when the change procedure allows backing out within a short time
- OS and supporting software updates (e.g. new major versions of SLF)
- Production application patches and minor upgrades or feature additions
- Any testing that requires or affects Lustre components that are in production

4. **Major Change**

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.

Build Approvals Required:

- 1) Group Leader or Designated Alternate
- 2) Enterprise Architect
- 3) Change/Release Manager

Go Live Approvals Required:

- 1) Group Leader or Designated Alternate
- 2) Enterprise Architect
- 3) Change/Release Manager

Guidance: Significant upgrades to software/hardware or its supporting packages, major configuration changes (environment or application specific), introduction of new storage media or software systems, and any other changes that affect a large number of users.

Examples:

- Major hardware or new hardware configuration changes and additions (e.g. addition or decommissioning of a cluster),
- Adding or upgrading the existing network fabric,
- Decommissioning major components (software, clusters, computer platforms, etc.)
- Introduction of new storage technology (e.g. ZFS, Lustre, etc.) into production

Approved By: Michael Kaiser
Amitoj G Singh

Change/Release Manager
Deputy Head - High Performance Computing