

## FermiGrid 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.

### 0. Introductory Remarks - Items not under Change Management

FermiGrid has an extensive program of research and investigation, to avoid conflicts between this and Change Management (CM), the Change Manager agrees that Change Management will not apply to non-production services (ganglia, fgtest\*, itb, etc.). Change Management shall only apply to the set of services that have been defined and agreed to be production services.

The Gratia service currently has significant changes that are "in flight" (Gratia-HP/HA). Change Management shall not apply to these services until they have completed the "in flight" deployments that are underway (current estimate is 23-Feb-2010).

FermiGrid has significant infrastructure dependencies on the CD BlueArc NFS Server Appliance. Change Management for these areas shall not apply until the BlueArc administrators are also "onboarded" to Change Management.

FermiGrid shares some infrastructure with FEF that impacts both FermiGrid and FEF operations. FermiGrid shall make a "best effort" attempt to manage this infrastructure under Change Management, but Change Management shall not fully constrain these changes until FEF is also "onboarded" to Change Management.

FermiGrid will shortly be operating the Fermilab Cloud Computing service (FermiCloud). The Change Manager agrees that the administration of this service shall fall under the "research and investigation" exclusion above.

### 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, are also categorized as work.

Items that fall under the "Work" category include, but are not limited to:

- Any automated process (typically run via cron), including:
  - Nightly yum updates and ~Monthly Kernel patches
  - Daily CA Certificate Updates
  - Hourly CRL Updates
  - VOMRS to VOMS synchronization
  - VOMS server mirroring
  - GUMS synchronization from VOMS servers
- Any scripted process, examples:
  - Adding GUMS user mapping (cf - cms VO remapping requests).
  - Adding a UNIX user (account) / YP changes.
  - Adding a VO from the OSG VO package.
- Security updates.
- Installation of one or more yum packages from the standard SL(F) repositories that are not known to negatively impact production services.
- Changes to disk quotas and/or BlueArc NFS mount points.
- Updates and changes to the FermiGrid service monitor & metrics infrastructure.
- Routine batch system administration activities:
  - Adding new worker nodes to a Condor or PBS cluster.
  - Changing user priorities and/or quotas
  - Definition of new queues.
- Configuration changes to services via standard web interfaces.
- Standard Gratia collector administration.
- SAZ - Administration:
  - Banning / Unbanning user, vo, role, ca.
  - Trusting / Untrusting user, vo, role, ca.
- Management of Grid Trust Relationships (approved by CExec).
- Any defensive action in the form of tcp wrappers, firewalls, SAZ banning, or removal of user accounts that is necessary to defend us from a denial of service attack.
- Adding additional mappings in GUMS
- Adding secondary certificates to VOMRS
- Adding users to groups, adding roles to users
- Adding users to (cdf) VOMS
- Updates and/or changes to Backup scripts.
- Standard system administration tasks.
- Routine minor fixes to startup scripts and/or configuration files.
- Temporary service or configuration updates of any service that is deployed under FermiGrid-HA

## **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    | Group Leader or Line Manager |

**Final Approval Required:**

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

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

Items that fall under the "Standard Change" category include, but are not limited to:

- VDT updates within a minor version (VDT 2.0.0 -> VDT 2.0.1)
- Condor updates within a minor version (Condor 7.4.0 -> Condor 7.4.1)
- Persistent service or configuration updates of any service that is deployed under FermiGrid-HA:
  - VOMRS server, service or configuration updates
  - VOMS server, service or configuration updates
  - GUMS server, service or configuration updates
  - SAZ server, service or configuration updates
  - Squid server, service or configuration updates
  - MySQL server, service or configuration updates
  - ReSS server, service or configuration updates
  - Gratia-HP/HA server, service or configuration updates
  - LVS server, service or configuration changes
- Updates to FermiGrid Risk Assessment, Security and Contingency Plans (approved by CSEXEC and/or General Computer Security Coordinator).
- Changes to virtualization configurations (memory, disk, #cpus, etc.)

### 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:

#### 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 | 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: Bug fixes to code, changes to code affecting only one of the ITIL processes, human factor refinements, or user interfaces. Verbiage changes to process, which are consistent with existing policy, and have a local impact on work practices.

Examples:

- Major or minor version VDT updates (VDT 1.8.x -> VDT 2.0.0)
- Major or minor version Condor updates (Condor 7.2.3 -> Condor 7.4.1)
- Major or minor version Gratia updates (Gratia 1.2.x -> Gratia 1.3.x)

## 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).

Examples:

- Adding a new authorization mechanism (example: Shibboleth).
- Deploying a new service under HA (example: Gatekeeper-HA).
- Change of GUMS and/or SAZ communication protocol (SAML -> XCAML)

Approved By: Don Petravick  
Michael Kaiser  
Keith Chadwick

Change Manager  
Change Coordinator  
FermiGrid Services Manager