Computer Security Operations 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 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.* 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 process and policy documents that are editorial in nature and do not materially affect decisions. 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:

- Entering/expiring URLs to the site proxies (automated via malware feeds)
- Entering/expiring URLs to the site proxies (manually)
- Authorizing access to proxy servers for members of CSO.
- Diagnosing and solving URL/site accessibility issues.
- Debugging incidents and problems in the production proxy servers (this may include enabling detailed diagnostics for some period and restarting service components in some instances)
- Adding monitoring that will not disrupt production proxy servers(the person making the change will include in the service ticket a statement about the change and how they believe it will not affect production)

2. Standard Change

Standard Changes are low risk, routine changes to the production system performed according to a template. 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. The group's standard maintenance window includes all normal work hours. Some standard changes are announced to users; others are coordinated with customers' representatives.

Examples:

- Entering/expiring categories to the site proxies
- Making configuration corrections/changes (such changes may be blocking malicious user-agents, modifying what ports are intercepted, etc.).
- Allocating more resources (e.g. adding proxy servers to the WCCP Pool).
- Firmware and supporting software infrastructure minor release patches and tuning
- Proxy server 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

3. Minor Change

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	Department level Line Manager
Approval to go live	Department level Line Manager

Final Approval Required:

Authorization to build	Pre-approved
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 that are either transparent to users or affect only a small set of users.

Examples:

- Minor hardware configuration changes.
- Significant firmware upgrades or OS configuration changes.
- Changes to APIs that affect supporting infrastructure (e.g. savory).
- Any testing that may affect changes to a single production proxy server (but not the pool).
- Decommissioning major components (software, network cards, etc.)

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.

Initial Approval Required:

Authorization to build	Department level Line Manager
Approval to go live	Department level Line Manager

Final Approval Required:

Authorization to build	Change Manager
Approval to go live	Change Manager

Guidance: Major changes are upgrades to application software 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 most customers.

Examples:

- Major hardware or hardware configuration changes and additions (e.g., something that impacts the production proxy server pool (all proxy servers))
- Major application upgrades, features, configuration changes and additions(e.g., something that impacts the production proxy server pool (all proxy servers))
- Introduction of new technology (e.g. switching vendors) into production

Approved By:	Michael Kaiser	Change Manager
	Arthur Lee	CSO Group Leader