“Computer Systems Quality and Compliance” discusses the quality and compliance aspects of computer systems, and aims to be useful to practitioners in these areas. We intend this column to be a useful resource for daily work applications.

Reader comments, questions, and suggestions are needed to help us fulfill our objective for this column. Please send your comments and suggestions to column coordinator Barbara Nollau at barbara.nollau@av.abbott.com or journal coordinating editor Susan Haigney at shaigney@advanstar.com.

KEY POINTS
In this issue of the column, the following key points are discussed:

- Change control as good business practice
- The importance of having a change control process in place
- Regulatory compliance drivers for change control
- Developing a change control procedure and process for computerized systems
- Determining the level of re-testing required
- Different types of change control and value in consistency.

INTRODUCTION
Change control is a common term describing the process of managing how changes are introduced into a controlled system. Experts agree that most problems of software and computer systems are introduced when changes are made either during development or during use of the systems. Change control is required to ensure that validated systems remain under control even as they undergo changes.

Changes to the system are likely to disqualify the original validation if not performed and tracked carefully. Lack of documentation for changes and testing after changes is one of the most frequently cited deviations during internal or external audits. A robust change control process must be in place to prevent unfavorable or non-compliant outcomes as a result of change to systems.
CHANGE CONTROL PROCESS

Computer systems are not static and they do require a robust maintenance program soon after the initial validation. A change control procedure is critical to ensure that changes are assessed, documented, performed, and tracked consistently across the organization. This procedure should define the process to be followed for assessing and implementing the changes.

The change control process is typically defined by proposing the need for the change, pre-approval and planning, executing the change, and final approval/implementing the change. Change completion is then documented. Figure 1 describes the change control process.

Proposed Change

The change requestor formally requests a change to the system (usually via a form or online entry point). Change requests need to be evaluated to ensure they are appropriate and that the proposed change will not negatively impact any other aspect or capability of the system. Then it should be determined whether the change should be classified as an emergency or routine change. Some companies also have a third category for non-essential changes that may be batched. This classification will indicate the required timing of implementation and associated activities. It is essential that the change control procedure provide an expedited pathway for emergency changes.

Often, emergency changes are needed to correct software problems or restore processing operations quickly. Although the changes must be completed in a short timeline, they must be implemented in a well-controlled manner. Emergency changes should be subject to similar controls as routine changes. However, the process may be abbreviated relative to the change request, evaluation, and approval to ensure changes can be made quickly. The process should be designed to ensure affected parties complete detailed evaluations and documentation of the emergency change(s) as soon as possible after implementation. Whenever possible, emergency changes should be tested prior to implementation. If IT is unable to thoroughly test emergency modifications before installation, it is critical that they appropriately backup files and programs as well as have a back-out plan in place.

Pre-Approval and Planning

A cross-functional team should determine how the change might affect the system before the change is made. This cross-functional team should include the system owner (or business area representative delegated by the system owner) and other key contributors including, but not limited to, quality assurance (QA) and IT. Depending on the nature and assessed impact of the change, the level and rigor of documentation and testing will likely vary.

Approval to move forward with the change must occur before any changes to the system are made. In an urgent situation (emergency change) a change might be granted prior to completion of the formal change control process. In that case, the type of change must be documented in the same manner. The decision whether to accept or reject a change would be based on a number of rules. The fundamental logic should be as follows:

- Is the change unavoidable?
- Does the change increase the overall benefit to the organization?
- Is the project team able to make such a change?
- Is the change best done now, or would it be more beneficial to defer it?
- Is the change going to impact other areas or systems?

An objective process should be in place to determine the magnitude and complexity of the proposed change as well as the level of impact it will have on the system. This understanding will lead to the determina-
tion of the required documentation rigor. This im-
pact determination will also help with determining
the level of testing required for the system. Some
companies categorize changes as major, minor, etc.,
which can enable more consistent decision-making
if each category is managed consistently.

By reviewing the original validation requirements
associated with the changing functionality and any
related functionality, and evaluating any potential
new risks that might be introduced through the
changes to the system, the focus and level of re-
testing can be determined. This is often referred to
as a regression analysis. Additionally, the Traceabil-
ity Matrix (TM) is a document that formally links
requirements to design and testing throughout the
validation process, and that can be a practical tool
to help determine regression testing as well.

The regression analysis would indicate the func-
tionality that requires regression testing as well as a
solid rationale for excluding those functions that are
not impacted by the change.

The following documents should be assessed for
potential impact due to the change, and updates
should be planned, where required:

- Validation package including user requirements
  specification (URS), technical requirements
  specification (TRS), TM, design qualification
  (DQ), installation qualification (IQ), operation-
  al qualification (OQ), performance qualification
  (PQ), and validation plan and report
- Design documentation
- Procedures for using and maintaining
  the system.

In some cases (e.g., for large or complex
changes, or due to cumulative change over
time), a complete rewrite of certain affected
documents may be necessary in lieu of ad-
denda or point revisions.

Changes should be planned and execut-
ed cross-functionally, minimally involving
IT, QA, and the business area owning the
system. Changes should be communicated
to all impacted areas and functions.

**Executing the Change**

In the execution phase, the change is actually made
in a staging environment so it can be tested before
production implementation. The change (and other
aspects of the system that may have been affected)
is tested to ensure the system accuracy, reliability,
and consistent intended performance. The test-
ing must be documented, and the results should
either lead to corrections and additional testing, or
confirm that the end result after the change is what
was intended. The documentation associated with
the change should also be completed.

Changes should initially be implemented away
from the production environment of the validated
system. This will ensure that no changes are made
to the production environment until they have been
fully qualified and found to be functioning as ex-
pected. Relative to computer systems, it is advisable
to have several virtual environments defined in the
architecture landscape. Typical environments are
described in Figure 2 and discussed as follows:

- Development environment (sometimes referred
to as “Sandbox”)—a virtual environment where
  experimental coding/configuration takes place,
as the developer/configurator is trying different
  solutions, doing preliminary unit testing, etc.
- System testing—a virtual environment used for
  preliminary systems testing conducted by IT
- Validation—a virtual environment that is fro-
  zen and representative of production, set up for
  validation testing, and controlled as unchange-
able throughout validation testing
- Training (not always used by all companies for

![Figure 2. Virtual environments.](image)
all systems)—a virtual environment used for hands-on training on the new or revised system.

- Production—the live business environment or “instance” of the system.

Testing should verify the following:
- System performs as expected after the changes were made
- System’s original functionality continues to work after the changes were made
- New changes do not introduce errors that keep the system away from performing as intended.

**Final Approval/Implementing the Change**

Final approval to release the new version to production is granted based on successful test results and completion of documentation package. If training is required, affected personnel (e.g., users, super-users, IT support) must either be trained before they are able to access and use the system or before the implementation into the production environment. Final approval is typically granted by the system owner and approval authorities from QA and IT. The new version of the system/software is then released to the production environment. This can be done via login script or other means.

It should be noted that in the event of an audit that includes inspection of any computer system used for a regulated purpose, inspectors will typically review the system documentation, including records of changes. This review will help them to determine the level of change and consistency in decision making and documentation, both within the system and across systems.

The change control documentation produced will demonstrate the ongoing validated state of the system. Changes must be controlled and well documented throughout the process.

**CONCLUSION**

The change control process is important to ensure compliance and avoid a potential risk and possibly a business liability. An objective decision-making process should be used to determine the level and complexity of the proposed change. The level of impact that the change might have should also be determined, and stemming from that, the required documentation rigor. Additionally, an objective process will enable consistent management of all types of changes.

A change control process is necessary to prevent inappropriate modifications or modifications that lead to adverse effects. Effective change control is an important aspect of maintaining the validated state of the system, enabling continuous improvement, and preventing compliance gaps.

**REFERENCES**


**ARTICLE ACRONYM LISTING**

- **DQ**: Design Qualification
- **IQ**: Installation Qualification
- **IT**: Information Technology
- **OQ**: Operational Qualification
- **PQ**: Performance Qualification
- **QA**: Quality Assurance
- **TM**: Traceability Matrix
- **TRS**: Technical Requirements Specification
- **URS**: User Requirements Specification

**ABOUT THE AUTHOR**

Farhad Forozesh has 13 years of experience in the pharmaceutical and medical device industry. Farhad is a senior validation engineer at Abbott Vascular responsible for coordinating validation activities (equipment/software validation projects) with all primary and support groups and providing technical leadership and guidance. Farhad can be contacted by e-mail at farhad.forozesh@av.abbott.com.

**ABOUT THE COLUMN COORDINATOR**

Barbara Nollau is a director of supplier and alliances quality at Abbott Vascular. She has 26 years of experience and increasing responsibility in the pharmaceutical and medical device industries, spanning the areas of manufacturing, quality assurance and compliance, validation, and information technology. Ms. Nollau can be reached by e-mail at Barbara.nollau@av.abbott.com.