



IT Change Management

Approved: July 25th, 2016

Implemented: July 25th, 2016

Contents

- 1. Definitions and abbreviations used in this document 3
- 2. Purpose: 3
 - 2.1 Involvement of the PPS’s CIO..... 3
- 3. Scope Inclusion 4
- 4. Scope Exclusion..... 4
- 5. Change Management Procedure 4
 - Standard Change Management 4
 - Emergent Changes 7
- 6. Technical Review..... 8
- 7. Update Planning..... 8
- 8. Change Implementation 8
- 9. Post Implementation Review 9
- 10. Closing the Change..... 10
- 11. Communication Plan 10
- 12. Education and Training 10
- 13. References 11

1. Definitions and abbreviations used in this document

PPS: Performing provider system

DSRIP: Delivery System Reform Incentive program

RFC: Request for Change

SCC: Suffolk Care Collaborative

Change Control: The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decision making, and approval of the change

Change Management: The Service Management process responsible for controlling and managing requests to effect changes to the IT Infrastructure, or any aspect of IT services, to promote business benefit while minimizing the risk of disruption to services

RFC: Request for Change

Change initiator: The change initiator is the person who initially perceives the need for the change and develops, plans, and executes the steps necessary to meet the initial requirements for a Request for Change (RFC).

CAB (Change advisory board): The change advisory board (CAB) is a body that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. When a CAB is convened, members should be chosen who are capable of ensuring that all changes within the scope of the CAB are adequately assessed from both a business and a technical viewpoint.

CMDB: Change Management Database

2. Purpose:

- To define a process for managing changes within the DSRIP program life cycle.
- Standardize policies and procedures which are used for efficient and prompt handling of all changes.
- Manage and minimize risk.
- Ensure all authorized changes support PPS needs and goals
- Minimize the severity of any impact and disruption to the IT systems, PPS business operations and system users
- To ensure change requests that arise following the requirements documentation process, are effectively communicated and managed.
- To ensure all projects comply with the defined policy and procedure to address changes to scope, requirements or design during the program life cycle.
- Provide documentation that enables PPS partners and stakeholders to understand the configuration of the IT environment at any point in time.
- Employ safeguards to maintain control of the IT environment.

2.1 Involvement of the PPS's CIO

The PPS CIO is the chair of the IT Governance committee and has participated in the review and approval of this document.

3. Scope Inclusion

Change management will be applied to any configuration item or element of the IT infrastructure that may impact interoperability and data sharing for more than one partner across the PPS. Types of changes include installation, alteration or decommissioning of hardware, software, network, system environment, procedure and data sharing specifications.

4. Scope Exclusion

Changes to a PPS partner's IT infrastructure or environment that does not impact PPS data sharing or interoperability across the PPS or considered part of the PPS partner's standard operating procedures.

5. Change Management Procedure

Standard Change Management

A standard change is a change to a service or infrastructure for which the approach is preauthorized by change management. A standard change has an accepted and established procedure to provide a specific change requirement.

The crucial elements of a standard change are that:

- There is a defined trigger to initiate the request for change.
- The tasks are well known, documented, and proven
- Authorization is given in advance.
- The risk is usually low and always well understood
- Budgetary approval considerations will be reviewed by the SCC IT Task Force and/or SCC IT Governance Committee.
- Approval of a standard change will be granted by the SCC IT Task Force

Standard IT Change Management Process Flow

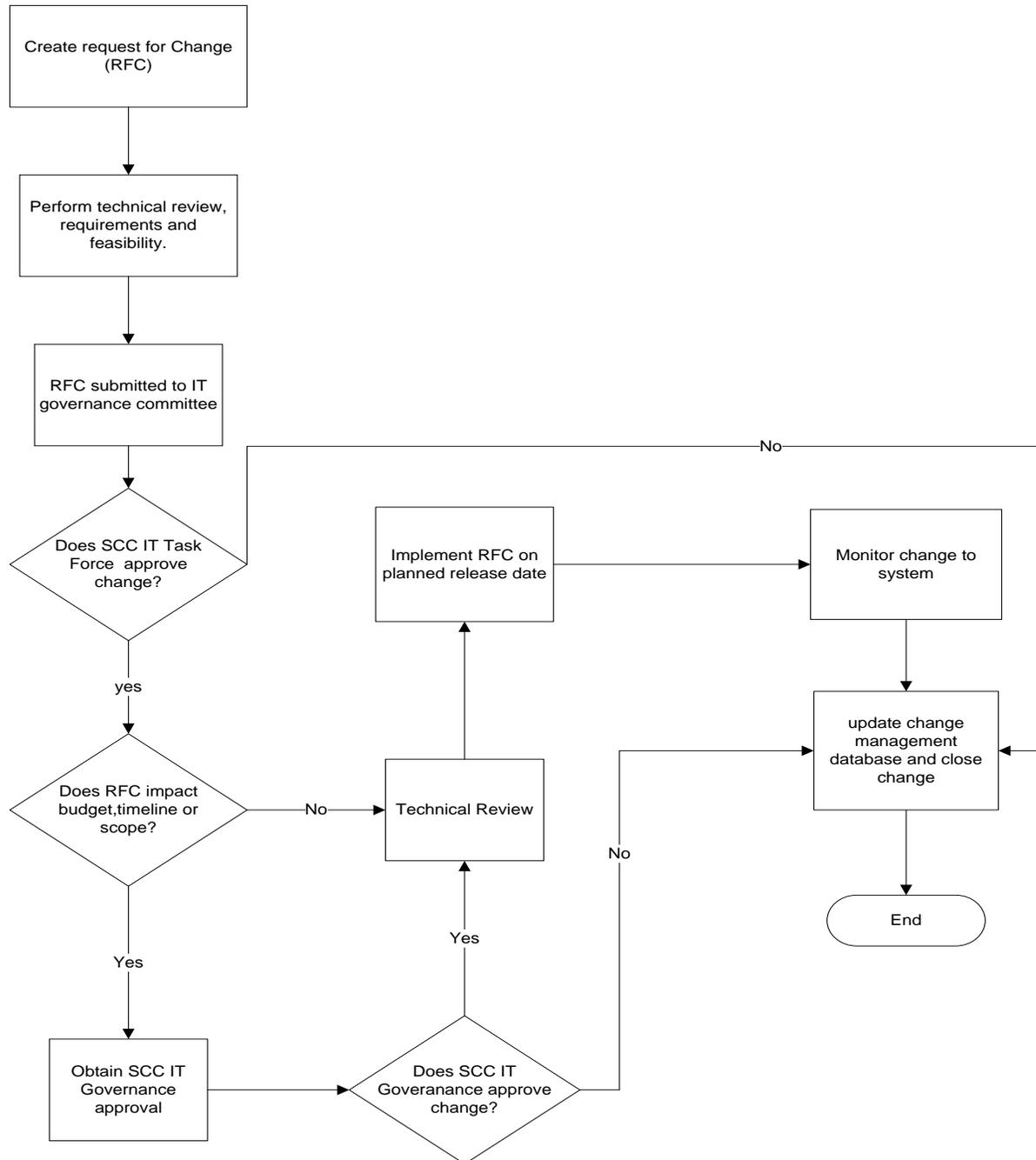
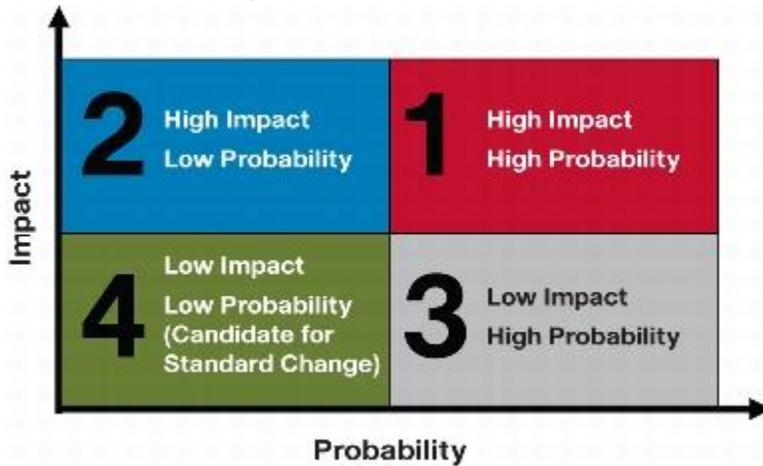


Figure 1. Standard Change Process Flow

The IT change management process will include the following standards to reduce potential impact to users and the system:

1. All IT related aspects of the Suffolk Care Collaborative projects shall adhere to the Suffolk Care Collaborative IT Change Management policies and procedures.
2. If the DSRIP Program Manager agrees to proceed with the change, the requestor will complete and submit the Program Change Management form.
3. All documentation supporting the change shall be submitted with the Project Change Management form.
4. The request for change will be documented by the change requestor using the approved change request form adopted by the PPS.
5. The change request form will be available on the Suffolk Care Collaborative Performance Logic website here -> <https://scc.perflogic.com>. All constituencies will be trained and empowered to request changes to the infrastructure.
 - All changes to a project's scope, requirements or design shall be addressed through the Change Management process once the Requirements document has been approved and the Requirements Phase of the Project Life Cycle has been completed.
 - All changes to the IT production system will have a corresponding set of documentation that describes the change and the business reason for the change for all routine and emergent changes. The Change management form will include the following items:
 - A description of the change.
 - The reason for the change.
 - The benefits of the change.
 - The requested date of the change.
 - The impacted facilities, departments or business units.
 - The impact on the project schedule.
 - The impact on the project budget.
 - The chronological order in which these steps should be taken, with any dependencies or co-processing will be identified in the RFC form.
 - The steps that should be taken to handle the change, including handling issues such as exceptions and unexpected events
 - Responsibilities; who should do what
 - Timescales and thresholds for completion of the actions
 - Escalation procedures; who should be contacted and when

- Risk and impact assessment of the requested change on scope, resources, budget and timelines. A simple Risk Assessment Matrix will be utilized to categorize the level of risk associated with the change.



6. The Program Change Management form shall be submitted to the SCC IT work stream Committee for review.
7. The SCC IT taskforce will review the change request in collaboration with the business units impacted by the change and approve or deny the change.
8. All changes that impact the project budget and/or schedule shall be reviewed and approved by the SCC IT Governance committee
9. The SCC IT Program Manager shall maintain the approved Project Change Management form, all associated documentation and disposition as a component of the project documentation. Here again all documentation will be stored in a centrally accessible SCC website at <https://scc.perflogic.com>.

Emergent Changes

Emergency changes may arise due to an incident which requires an initiated response to a critical IT situation. This may be an incident or problem requiring immediate action to restore service, prevent service disruption or patient safety in nature. Emergent changes should be designed carefully and tested before implementation. Details of emergency changes may be documented retroactively to be submitted back to the IT governance and SCC board as informational.

The number of emergency changes proposed should be kept to an absolute minimum.

The emergency change category is reserved for changes where:

- Users are unable to perform critical functions on the system.
- A fix is required to repair a service negatively impacting the business to a high degree
- A potential patient safety risk is identified.
- A back-out of an attempted change is unsuccessful.

The emergency change procedure will follow the normal change procedure except that:

- Approval will be given by the emergency CAB (ECAB) rather than waiting for a CAB meeting.
- Documentation, such as updating the change record and configuration data, may be deferred, typically until normal working hours.

6. Technical Review

Prior to submitting the RFC for CAB review, each RFC must undergo a technical review. This review checks the following aspects of the proposed change:

- Correctness of all technical information, including preparation, implementation, verification, and back-out procedures
- Completeness of change, testing procedures, and documentation
- Feasibility of the change
- Potential side effects and impact on other services or infrastructure
- Worst-case impact (both change and back-out procedure fail)

This review is performed by the technical resources familiar with the area affected by the change as well as other technical resources with general knowledge of the subject. Where applicable, the Information Security Officers must review any changes that may impact system security or handling of PHI data across the PPS. The authorization following the technical review is a formal sign-off recorded in the change management database.

7. Update Planning

Changes will be grouped into scheduled release dates. Changes will be performed on Tuesdays of the week. The changes may be designed, tested, and released together if the amount of changes involved can be handled by DSRIP partners and its end users.

Major releases may need to be scheduled with the business and stakeholders at a predetermined time. Wherever possible, change management should schedule authorized changes into target release or deployment packages and recommend the allocation of resources accordingly.

The CAB will coordinate the production and distribution of a change schedule and projected service outage, if applicable, in collaboration with the IT subject matter experts. The change schedule contains details of all the changes authorized for implementation and their proposed implementation dates. These documents are agreed upon in advance with the relevant customers within the business, service-level management, the service desk, and with availability management. Once agreed upon, the Suffolk Care Collaborative will use established procedures to communicate any additional downtime that will result from the change to the PPS community.

8. Change Implementation

Authorized RFCs will be passed to the relevant technical groups for building of the changes.

The following tasks are performed during this stage:

- Technical review of the change.

- Build the change
- Pre-test the change
- Complete change deployment plan
- Implement the change
- Test IT infrastructure post-change

Remediation procedures should be prepared and documented in advance for each authorized change so that if errors occur during or after implementation, these procedures can be quickly activated with minimum impact on service quality. Authority and responsibility for invoking remediation is specified in advance in the change documentation form.

In certain scenarios a phased implementation approach may be necessary. This may include starting with a small pilot in the production environment until the behavior resulting from the change can be established. Once observations are made and confidence increases, additional phases can be rolled out.

Testing may continue in parallel with early live usage of a service-looking at unusual, unexpected, or future situations so that further correcting action can be taken before any detected errors become apparent in live operation.

The implementation of such changes should be scheduled when the least impact on live services is likely. Support staff should be available to quickly respond to any incidents that might arise.

9. Post Implementation Review

On completion of the change, the results should be reported for evaluation to those responsible for managing changes, and then presented as a completed change for stakeholder agreement (including the closing of related incidents, problems, or known errors).

A review should also include any incidents arising as a result of the change (if they are known at this stage). If the change is part of a service managed by an external provider, details of any contractual service targets will be required (for example, no priority 1 incidents during the first week following implementation).

A post-implementation review (PIR) should be carried out to confirm that the change has met its objectives, that the initiator and stakeholders are satisfied with the results, and that there have been no unexpected side effects. Lessons learned should be factored into future changes.

Change management must review new or changed services after a predefined period has elapsed. This process will be incorporated into the standing SCC IT Task Force meeting as a standing agenda item. The purpose of the review is to establish that:

- The change has had the desired effect and met its objectives
- Users, customers, and other stakeholders are content with the results (if not, the review should identify any shortcomings)
- There are no unexpected or undesirable side effects to functionality, service levels, or warranties, such as availability, capacity, security, performance, and costs
- The resources used to implement the change were as planned
- The release and deployment plan worked correctly (the review should include comments from the implementers)

- The change was implemented on time and to cost
- The remediation plan functioned correctly, if needed

Where a change has not achieved its objectives, the IT Task Force should decide what follow-up action is required, which could involve raising a revised RFC. If the review is satisfactory or the original change is abandoned (for example, when the circumstances that required the change are no longer current and the requirement disappears) the RFC should be formally closed in the logging system.

10. Closing the Change

All approved, pending, completed and denied change requests will be managed and stored on the SCC Performance Logic website <https://scc.perflogic.com>.

The change success, failure, related plans, etc. are communicated to all stakeholders by email notification. Standard distribution lists will be created and utilized wherever possible.

11. Communication Plan

The PPS hub leads; Stony Brook Medicine, Northwell Health and Catholic Health Services are responsible for communicating and assessing IT system changes with its downstream PPS partners. The hub leads must assess that IT changes will not impact interoperability and data sharing downstream or the ability for the downstream partners to send data to the hub lead or PPS.

A PPS partner is not required to submit a change control to the SCC when performing a system upgrade or replacement to its own systems. However it is the responsibility of the hub leads to work with its downstream partners to assess if such changes will negatively affect the PPS partner from sending data to the hub lead and/or PPS lead as well as interoperability with the RHIO.

12. Education and Training

For changes that impact end users of Cerner's Enterprise data warehouse, Cerner has a forum to communicate code changes, upgrades, and newflashes specific to each solution. Client representatives are asked to subscribe to the solution specific HealthAnalytics Community uCern to obtain updates: <https://connect.ucern.com/groups/healthedw-healthanalytics-community>.

Cerner outlines specific training agreements in respective Sales Orders. Cerner's overall approach to HealthEDW training is focused on maintaining HealthIntent platform concepts and processes, data validation and security; report writing using both Tableau and Business Objects; and working with standard reports. Cerner deploys a "Train the Trainer" model for training the lead organization representatives, and includes client-facing training materials. Training events will be requested and managed through the client's Cerner assigned Engagement Leader. The client assumes responsibility for future training of downstream partners and their representatives

For changes beyond Cerner's standard Enterprise Data Warehouse features, the SCC will notify its partners of new features and functions related to interoperability and data sharing via monthly email newsletters. This may include such features as newly developed reports, changes in data mining capabilities, or enhanced ways to evaluate PPS data.

As a general statement this document represents the SCC's Change Management Training material. As of the date of this writing each hub lead representative has either co-authored or been trained on the Change Management Strategy. Each Hub lead is in turn responsible for assuring training is completed within their individual organizations and downstream partners if applicable.

13. References

1. ITSM Community <http://www.itsmcommunity.org/Resources/templates>
2. Change Management Best Practices www.cisco.com
3. Stickel, Edward. Change control vs. Change Management: Moving Beyond IT
<http://www.technologyexecutivesclub.com/Articles/management/artChangeControl.php>