I2R System Stabilization Tiger Team
Change Control Track
Summary Report

Author(s):	Melissa Liu
Contributors:	Danny Liu, Logan Wilkins, Sherman Chiu, Moe Jabri, Iain Campbell, May Tran, Zach May, Trey Morris
Status:	Final
Date:	March 25, 2014

Table of Contents

1. Document Introduction

An analysis of P1 and P2 Alliance cases for I2R systems was conducted in the spring of 2006. Change management issues were identified as a critical area contributing to P1 and P2 cases, and as a result, work commenced to improve change management for I2R. This document describes the work and results of that team.

2. Executive Summary

A systematic analysis of P1 and P2 Alliance cases for CACO-managed I2R systems was conducted in April/May 2006. The case data covered the period from August 2005 through March 2006. The case analysis concluded that 35% of the P1/P2 cases were due to specific change management issues. Key issues were: impact assessment and test planning (18%); change control, release planning, and other issues (12%); and infrastructure change control issues (5%).

Due to schedule availability of key stakeholders, the P1/P2 case analysis readout was not conducted until the end of May. A "Get Well Plan" to address change control and other critical stability issues began to be defined in June. Getting teams in place took a significant period of time. The initial Change Control and Case Management teams were staffed in late July; the C3 Performance team lacked critical resources until late August. Staffing remained a problem throughout the program duration as resources were shifted and replaced multiple times, delaying the work of the teams. The teams stayed in place until December.

Prior to the work of the team, the C3 system had fairly weak change control practices; non-C3 systems had no formal change control. It was determined that improved impact assessment practices could not be ensured without a level of control to enforce them. The key focus for the team was therefore change control supported by formal risk and impact assessment.

Interim "stop-gap" measures were taken to reduce change-based risk: director-level approval for all I2R application changes (June); gatekeeper review for all I2R application changes (July); executive-level approval for all I2R application *and infrastructure* changes (August); addition of high-priority (for TS) non-I2R tools to I2R change control scope (September).

Based on interim results, the change-related P1/P2 failures were reduced by about half by the end of the program; from about 8 per month to about 4 per month. After those improvements, the cases in Q107 were overwhelmingly due to infrastructure change management issues (69%).

The interim change control process, while significantly improving outcomes, had some glaring inefficiencies. The Change Control Board (CCB) review meeting required a large number of people to sit through the meeting for 90 minutes on an almost-daily basis. Each request was discussed in a somewhat ad-hoc manner during the meeting. Requesters frequently had to attend multiple meetings before their requests were reviewed. Three executives had to review every change proposed, including both those CCB recommended approving, as well as those CCB recommended rejecting.

The "1.0" Change Control process to be deployed in December furthers the original change control improvements while addressing inefficiencies in the interim process.

A key addition to the 1.0 process is a formal Risk Assessment process framework. This process formalizes the ad-hoc change review and analysis formerly conducted in CCB, defines specific criteria driving change risk, specifies risk-based change governance, and defines a Risk Analyst role to conduct the analysis at specific points in the PLC process. The Risk Assessment process takes input from IT change requesters at specific points in

the PLC, adds external factors such as system priority and stability history, and uses criteria and weights to calculate a change risk rating. In addition, the analysis includes a summary of key change risks, implications, risk/benefit relationship, and any relevant impacts or implications from Architecture Review Board (ARB) sessions. The Risk Assessment process is linked to both the level of change control governing each change, as well as the test planning and execution that will validate the quality and readiness of the change.

The addition of the Risk Assessment framework enables the CCB decision body to be significantly scaled back, as key change analysis will be performed prior to, and as in input to, CCB decision meetings. Many person-hours can be saved with this change; in addition, the Risk Assessment process provides a consistent framework for evaluating and comparing changes.

Final results against the 1.0 process are pending implementation of the process in December, subsequent to this report.

Remaining Work

One key open item from this effort is the need to finalize interaction with Infrastructure Change Management practices currently under review. For the December go-live, the I2R change management process for Infrastructure and non-I2R tool changes will remain largely the same, with the exception of a requirement for earlier engagement (i.e., not immediately pre-deployment) with the CCB for planned projects.

Other remaining work includes completion of changes to Kintana approvers for better enforcement of the change control process, and support for the corporate-wide OnePCC deployment in 2007, which will improve tools enablement for the new process.

Recommendations for Next Steps

Suggested areas for further process improvement include:

- In-depth audit and improvement of QA processes (gatekeeper, test strategy/planning, knowledge retention)
- Development of additional I2R business system architecture documentation to facilitate impact assessment and test planning activities
- Improvement of IT project prioritization, funding, and resourcing practices to enable better decision making and alignment of resources with priorities
- Natural process evolution of the 1.0 process, including risk assessment and change governance tuning over time

3. Overview

The I2R System Stabilization program (also called the "I2R Get Well Plan") was defined in July 2006. Some initial steps were performed prior to that, including a system change "lock-down" communicated June 21, 2006. The Change Control effort was a sub-team within the overall I2R System Stabilization program. The background of the program and of the Change Control sub-team are described in the sections below.

3.1. Introduction to the Stabilization Tiger Team

In late 2005 and early 2006, system outages for I2R systems were at a high level (e.g. above 10 during a number of weeks), increasing, and volatile. At the time, not much was known about key causes, areas of greatest problems, and improvements needed. Although root cause analysis (RCA) was and is still performed for each case, conclusions tended to be focused on each case at hand, rather than looking across cases to identify key themes and trends.

An analysis of P1 and P2 Alliance cases was conducted in April 2006 to identify the causes of the level, upward trend, and volatility of these cases and the key actions needed to address them. The analysis used case data from August 2005 through March 2006. Due to scheduling constraints, the actual review of the results did not take place until late May.

3.1.1. Results of P1/P2 Case Analysis

At the time of the analysis, 35% of the cases were related to change management issues. Of that 35%, the key areas were:

- Impact assessment, test planning, and test execution: 18%
- Change control, release process, and other issues: 12%
- Infrastructure configuration changes: 5%

Other key issues were the fact that recurring bugs were not getting addressed (12% of cases overall), and the fact that performance problems were increasing due to lack of proactive maintenance functions, such as capacity planning and proactive data management (e.g., data archive/purge/retention policies). One other area causing a surprisingly high (compared to standard) number of outages was the category of hardware failures. Two possible causes were noted: large number of failure points, due to a very large number of applications in use; or lack of proactive maintenance actions to replace hardware components before they fail.

Two-thirds of the cases were on non-C3 systems (for example, Software Center). However, the business perceived the only C3 system to be unstable. The non-C3 applications with the most frequently-occurring outages were: Tablebuild (9% of the original caseload); <company>Live (8%); SFA (7%); SIPS (5%); CaseKwery (6%); C3 business layer (not considered part of C3 by the support organization-5%); Topic/Google (5%).

Of the C3 cases, the most frequently-occurring areas were: B2B (18% of C3 cases); SVO (11%); TSRT Query (9%).

Seventy-two percent of the original cases were business-impacting, with two-thirds of those classified as case severity S3.

3.1.2. Objectives

The objective of the I2R System Stabilization program was to improve the stability of I2R systems by addressing key causes of outages.

3.1.3. Program Tracks

Two program tracks were initially defined: Change Control and Performance. A third track was added based on very visible failures in Case Management (for example, two highly visible P1/P2 case outages were stalled for roughly 24 hours before being routed to the right IT organization to address them).

Track leadership and team membership changed many times over the course of the program, extending the program's planned duration. Final team leadership was as follows:

- Change Control – Iain Campbell (SBS) and Danny Liu (I2R-IT)
    - Formerly Logan Wilkins, Ed Freeman, Ryan Schmierer
- Case Management – Chris Thomas with Igal Zadkovsky (both CACO)
- Performance – Rajiv Wani (SIS) with Jyoti Sarin (I2R-IT)
    - Formerly Ed Freeman
    - This team was not staffed until late August
- Program – Stephen Liem (I2R-IT). Supported through September by Melissa Liu, then by Rodney Rowell

3.2. Change Control Track

Background on the Change Control track of the program is provided below.

3.2.1. Team Mission and Objectives

The mission of the change control team, as stated at the September 28 executive review was to:

> *Define and institute a process to minimize change-related failures in critical I2R business-impacting tool systems and lay the groundwork to measure the outcomes of the process*

During the conduct of this team, much more attention was focused on the process improvements needed to address the gaps than on the measurements needed to measure the outcome. However, suggested metrics are included in Section 10.

The articulated team objective was as follows:

> *Control changes to IT applications, tools, processes, roles and infrastructure with minimal negative impact to critical I2R business processes*

Specific team goals:

- Develop and deploy an updated change control process that meets the objective
- Develop recommendations, policies, and efficient processes
- Enable a sustained focus on systems quality and stability, particularly with regard to managing the impact of changes introduced to those systems

3.2.2. Guiding Factors

Several guiding factors drove the definition of the revised change control process:

- The process should fit into and interact with the existing process structure (<company> PLC process, existing tasks, deliverables, and responsibilities)
- The process should be efficient, with degree of change control corresponding to level of change risk, e.g., not overly burdensome and resource-intensive for small, low-risk changes
- The process should be sustainable, i.e., not requiring huge amounts of resources and time for compliance
- Where possible, existing tasks, deliverables, knowledge, responsibility should be leveraged
- The process should be able to scale to manage all I2R changes, and potentially all CA changes

3.2.3. Team

The Change Control team was in place from late July through December, 2006. During that time, team membership – and leadership – changed many times, hindering and in some cases stalling forward momentum. The final team was able to restart team activity and get significant effort focused on completing the work of the team.

The team consisted of the following members:

Team Member	Role
Iain Campbell (SBS)	Team Co-lead (final) CCB and SBS representative
Sherman Chiu (I2R-IT)	Risk assessment and process definition

Team Member	Role
Ed Freeman (I2R-IT)	Identified Team Lead (September) Never became active team lead due to unplanned PTO and other factors
Blair Helsing (M-Squared Consulting)	Infrastructure, metrics, risk assessment (October)
Moe Jabri (CA-QA)	QA representative
Danny Liu (I2R-IT)	Team Co-lead (final)
Melissa Liu (PRTM)	Subject matter expert: Change control history and issues; change control best practices Risk Assessment (mid-November) Summary report author
Zach May (I2R-IT)	Tool support (Kintana)
Trey Morris (SIS)	SIS and ARB representative Process flow documentation author
May Tran (I2R-IT, SOX)	Kintana, OnePCC, PCC/SOX subject matter expert
Ryan Schmierer (CACO)	Original Team Lead Executive Review Board subject matter expert Original CACO team representative
Logan Wilkins (I2R-IT)	Team Lead (late September-early October) Team Advisor (post early October)
Randy Wolfgram (SIS)	I2R representative for Infrastructure Change Management meeting (identifying CRs of interest to I2R)

3.2.4. Starting Point for Process Improvement

At the outset of this program, I2R-IT did not have a standard change control process. The change control board (CCB) governed changes for the C3 system only. There was no formal change control mechanism in place for non-C3 systems. The Kintana tool, used for source code migration to Production and Stage environments, could have enforced some degree of change control; however, non-C3 approvers frequently were the development teams themselves.

There was no formal method for assessing the risk and impact of changes for either C3 or non-C3 systems. Impacts of changes were often not understood until after the change was made and negatively impacted a dependent component.

Little I2R system architecture and system interface documentation existed that could support impact assessment. EMAN was used to manually maintain application dependencies and was frequently found to be missing dependencies[1]. A few diagrams were created at the outset of C3 implementation and described C3 interactions with other systems. Not all interactions were reflected on the diagram. No architectural documentation was noted for non-C3 systems. Upstream and downstream dependencies were noted in the application repository where known, but the dependency information was known to be incomplete.

The I2R organization had little insight into, and less control over, infrastructure changes with the potential to impact I2R systems. Infrastructure issues were a frequent cause of I2R outages. Infrastructure organizations supporting I2R were engaged in a mostly reactive model; little proactive maintenance was in-place. No service level management operating agreements were noted between I2R IT organizations (including CACO) and the infrastructure IT organizations that supported them.

There was no visibility into or control over changes to non-I2R tools that were critical to the I2R business function (e.g., MeetingPlace). The CACO I2R support organization (CACO) did not have visibility into outages for those tools.

A few transitions occurred during this project: the transition of enhancement work from CACO to the IT teams; and the transition of test responsibilities from CACO and the IT teams to the CA-QA organization. Neither transition was complete at the time this project concluded.

3.2.5. Team Focus Areas

Based on the initial case analysis, the key focus areas for the Tiger team were:

- Risk and Impact Assessment, specifically the link between change risk and both test strategy and level of change control
    - Supporting this focus required definition of a risk assessment framework, inputs into and classification of levels of change risk, and identification of the “right” level of control for each level of risk
- Change control, both through a control forum (CCB) and through tool support to enforce change control (Kintana)
    - In the original case analysis, change control was a less significant root cause area than impact assessment; however, control was required to ensure the appropriate assessment and testing was performed and was therefore a necessary prerequisite

For the above areas of focus, the team identified approaches for I2R-managed applications as well as critical I2R-impacting tools and infrastructure.

[1] In any event, EMAN dependency information records which systems a particular system interacts with; it does not record *how* those applications depend on or interact with each other. Complete EMAN dependency information could only be used to identify *candidate* systems affected by a change.

The team did not focus specifically on change issues related to release processes (for example, identified gaps in release playbooks). These issues decreased significantly after implementation of the major/minor C3 release cycles. No cases were noted from mid-January until the September release (the September release did have a few release process issues). RMO maintains responsibility for identifying and addressing issues in these areas.

Metrics were to be defined by the team; however, the high rate of team turnover prevented this area from ever being a significant emphasis. Definition of the core process tended to take higher priority when resources were lost or shuffled.

3.2.6. Results

Interim "stop-gap" measures were taken to reduce change-based risk: director-level approval for all I2R application changes (June); gatekeeper review for all I2R application changes (July); executive-level approval for all I2R application *and infrastructure* changes (August); addition of high-priority (for TS) non-I2R tools to I2R change control scope (September).

Based on interim results, the change-related P1/P2 failures were reduced by about half by the end of the program; from about 8 per month to about 4 per month. After those improvements, the cases in Q107 were overwhelmingly due to infrastructure change management issues (69%)[2].

Final results against the "1.0" Change Control process are pending implementation of the process in December, subsequent to this report. Metrics have been defined that will assist in measuring both outcomes and progress toward process adoption; these metrics are included in Section 10.

[2] Details of Q107 change-related P1/P2 cases can be found at:
http://workspace/Livelink/livelink.exe?func=ll&objId=18639273&objAction=Open

4. New Process Introduction

This section provides background information on the new process. The following sections describe key aspects of the new process in more detail.

4.1. Scope

The revised change control process governs changes to *all* I2R applications, whether through releases, projects, tacticals, release exceptions, or Emergency Bug Fixes. In addition, the process governs changes to I2R-impacting infrastructure and non-I2R "Top X" tools. The change management approaches for each of these situations varies; each scenario is described in Section 7.

4.2. Intermediate Steps Taken

Prior to the December rollout of this revised process, a few steps had been taken to make immediate improvements to change control for I2R systems. The interim steps are listed below:

- Incorporated non-C3 I2R systems into change control process (June)
- Added a QA gatekeeper role to ensure testing completed satisfactorily and with sufficient documentation, later combined with SOX gatekeeper into single role and area of coverage (July)
- Incorporated infrastructure-level changes for I2R systems into change control process (August)
- Instituted an "Executive Review Board" (ERB) to review and approve (or reject) all proposed system changes, including those planned into releases (August)
- Communicated change priorities and used those priorities to drive both change review discussions and change approval decisions (August)
    - Priorities specified by executive sponsors and supported by the business were:
        1. Changes to improve stability
        2. Changes to improve performance
        3. Changes critical to TS Initiatives
        4. All other changes
    - These priorities are expected to remain as specified (i.e., after the Tiger Team exits and the ERB is disbanded)
- Incorporated critical "Top X" tools outside of direct I2R control into change control process (September)

4.3. Summarized List of Process Changes

For ease of understanding the specific changes made to the change process, a summarized list of changes made from the prior change process is provided below.

- Added an iterative risk assessment process to ensure impacts and risks of changes are adequately identified and mitigated through testing
- Defined a Risk Analyst role to drive the risk assessment process and perform key analysis steps for it, including recommendations to CCB
- Added a Test Strategy document to connect identification of risks and impacts to an identified strategy to mitigate them to the extent needed
- Defined levels of change control and governance based on identified change risk
- Added a CCB authorization step prior to Execute Commit (EC) for a project or release; Authorization confirms the change window as well as informing requesters as to the governance path (level of change control) for the change
- Formalized a Test Plan review forum and approvals to ensure that test details are formally discussed and issues addressed
- Linked ARB review to Risk Assessment process and Test Strategies and Test Plans
- Made Stage migration for planned release changes an RMO responsibility, rather than CCB
- Requested earlier (Analysis phase) engagement from Infrastructure and non-I2R critical ("Top X") tools IT organizations for planned projects

4.4. Process Description Organization

The revised change control process was designed to fit within the <company> PLC process. No major PLC milestones (CC, EC, etc.) were added or deleted. In some cases, additional entry criteria *were* added.

This document assumes knowledge of the standard <company> PLC; no attempt will be made to fully describe the existing lifecycle within this document. Instead, the documentation will focus on describing how process changes *fit into* the PLC: new steps, new deliverables, new/revised entry/exit criteria, new relationships between existing steps and deliverables, etc.

The remaining sections describing the new process are organized as follows:

- Roles and responsibilities within the new process
- Overview of the Risk Assessment framework
- Details for specific change scenarios (e.g., Projects, Emergency Bug Fixes)
- Details of the revised I2R Change Control Board (CCB)

5. Roles and Responsibilities in the New Process

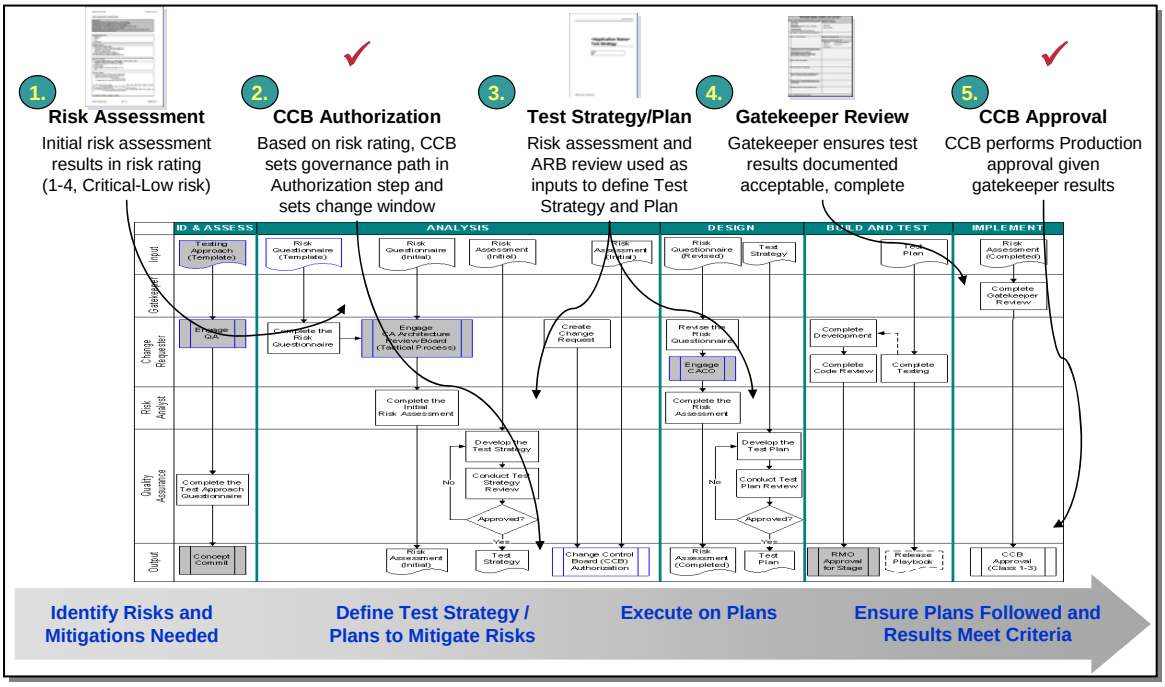
Role Name	Responsibilities
Architecture Review Board (ARB)	• Review change requests (both tacticals and projects) from an architectural perspective • Provide technical feedback and consultation to ensure that standards are met and best practices utilized; identify re-work needed, if any
Business (frequently working with / through SBS)	• Determine business prioritization of projects and tacticals • Fund IT projects and organizations to adequately support prioritized changes and system support and maintenance • Define system priorities • Review test documentation (Test Strategies, Test Plans, Test Scenarios and Test Cases) to ensure adequate coverage of business' quality concerns • Participate in User Acceptance Testing as defined in the test approach, test strategy, or test plan documentation • Ensure formal business sign-off (or rejection) is recorded for all system changes through attendance at release Readiness Review meetings
Business Approval Councils (BACs)	• Define priorities and severities for tactical changes • Provide input to release scope for tacticals to be included in major and minor releases
CCB	• Identify how specific changes will be governed through the change control process, based on change risk • Authorize and approve changes • Reject or redirect changes if more information is needed, if key risks need to be addressed, or if change risks outweigh the benefits.
Change Requesters	• Submit change requests • Ensure that system changes follow the change control and release processes • Complete Risk Questionnaires during Analysis (initial) and Design (revised) phases • Provide additional information regarding the change to Risk Analyst and CCB as requested • Ensure CA-QA is involved in testing the changes • Engage the Architecture Review Board (ARB) as defined in the ARB engagement process • Provide information required for Gatekeeper review

Role Name	Responsibilities
Gatekeeper	• Review test documentation, including testing performed, results compared to expected results, etc. for completeness, accuracy, and acceptability of results • Identify whether changes meet pre-defined gatekeeper criteria for readiness • Communicate and document gatekeeper decision to support production deployment approval (or non-approval)
Infrastructure IT	• Identify infrastructure changes with potential I2R impact • Engage the I2R CCB in the Analysis phase for planned projects with potential I2R impact
QA	• Define testing approaches required to ensure system changes meet business and quality requirements • Define test scenarios, test cases, and expected results • Execute testing, document testing performed, and identify discrepancies between actual results and expected results • Gauge readiness of system changes based on pre-determined criteria and results
Risk Analyst	• Assess risks of specific changes (projects, tacticals, release exceptions, etc.) based on risk factors such as type and complexity of change, system stability history, and system priority
RMO	• Define IT roadmap on an periodic basis, including IT projects and timeframes • Define proposed release scope (projects and tactical changes) for major and minor releases • Manage delivery of releases • Manage Stage approval for changes included in planned releases
Scope Change Boards (SCBs)	• Ensure changes to the scope of a release are controlled using a formal decision structure • The Release Manager owns the responsibility for forming an SCB if one will be used (SCBs are currently used for C3 releases only)
SBS	• Work with business organization to prioritize system changes and systems overall • Work with business to ensure IT funding is consistent with change and application priorities • Support and facilitate communication between IT and business

6. Risk Assessment Framework

One key component of the revised process is a formalized Risk Assessment framework. The key objective of the risk assessment process is to ensure that risks associated with specific change requests are identified, are used to drive the level of governance over the change, and are mitigated thoroughly through testing. In addition, the risk assessment will weigh the benefits of a change against its risk. If a change's risk is higher than the benefit that will be experienced from the change, the I2R change control board (CCB) may reject the change.

An overview of the risk assessment framework is provided in the diagram below.



6.1. Risk-based Change Governance

The governance path for a change is set at the CCB Approval review that occurs in the Analysis phase prior to Execute Commit (or Release Commit for tactical releases)[3]. The governance path is based on the change risk as assessed by the Risk Assessment. The Risk Assessment uses factors such as the following:

- Type and complexity of the change
- Complexity of system or application
- Priority of system or application
- Stability history of system or application (new applications are assumed to be unstable until there is enough history to properly categorize them)
- Impacts to other systems or applications

[3] See Section 7 for specific timing details for Projects, Tacticals, Release Exceptions, Emergency Bug Fixes, and Infrastructure changes

Based on the risk factors, a Risk Rating (formerly called the "Change Class") is produced. Risk Ratings, with examples, are provided below:

Risk Rating	Risk Level	Examples
4	Low	GUI change, Code, Configuration, Data Change, Business Configuration High comfort level and can be rolled back Minor changes to low priority application
3	Medium	Minor changes to critical application Detailed changes to non-critical application Application has history of stability High comfort level on change
2	High	Minor to moderate changes to critical application Non-critical application, but has history of instability Low to moderate <company> customer impact
1	Critical	Complicated changes to critical application History of instability Impacts and dependencies extensive or uncertain High <company> customer impact

Default governance guidelines for each level of identified risk are detailed below. CCB has full discretion to determine that specific changes require a higher level of governance than the minimum level indicated below, based on other factors.

	Governance Event	Classification Model	Risk Rating
Risk Analyst	Risk Assessment	Risk assessment done for all change risk levels, but level of detail depends on the Risk Rating	All
CCB	Authorization	CCB Authorization required for all changes	All
	Stage Approval	CCB Approval for stage required for release exceptions (RMO approval for all releases)	All
	Production Approval	CCB Approval for production required only for higher Risk Ratings	3 through 1
ARB	Tactical Review	Single architecture review point for tactical changes	All
	Initial Architecture Engagement	Initial review required for all project-level changes of all Risk Rating levels	All

	Governance Event	Classification Model	Risk Rating
	Primary Architecture Review	Secondary project-level review required for higher Risk Rating levels	3 through 1[4]
	Design Review	Final project-level review required for higher classes. High touch ARB required for highest level of Risk Rating for projects	2 and 1[5]
QA	Full Engagement	Currently "one size fits all" – may be modified post-Tiger Team	All
Gate-keeper	Full review	Gatekeeper requirements not currently scaled to size of change	All

The CCB will determine the governance path within the CCB meeting and will communicate that path, along with the change approval decision and change window as part of the CCB communication logistics[6].

[4] Risk Ratings and ARB designation as Low-, Medium-, or High-Touch may not correspond perfectly for every change. The ARB designation drives the number of ARB engagements; however, the Risk Ratings shown should in most cases correspond to those levels of ARB review.
[5] See footnote above.
[6] See Section 8 for details on the Change Control Board membership, logistics, communication, etc.

7. Specific Change Scenarios

There are five change scenarios documented in the sections below:

- Projects
- Tactical (smaller) changes
- Release Exceptions
- Emergency Bug Fixes (EBFs)
- Infrastructure and non-I2R tool changes

Projects generally refer to larger system changes that appear on the IT roadmap. Sometimes these changes are called “CFPs” (for “Client Funded Projects”). Projects are generally captured in the EmPower software tool.

Tactical changes generally refer to smaller, short-lead changes that are included in planned releases. C3 minor releases usually (but not always) consist only of tacticals. C3 major releases include projects as well as tacticals. Tactical changes are frequently captured in the I2R request tool. Occasionally the TestDirector tool is used to capture operational issues intended to be addressed in tactical fixes[7].

Although changes are generally bundled into planned release windows, specific changes may be designated as release exceptions. Release exceptions refer to changes that are deployed in between planned releases.

Emergency Bug Fixes (EBFs) are immediate changes to address outstanding P1 or P2 Alliance cases (i.e., system stability issues) that are interfering with the operational status of a system.

Infrastructure and non-I2R tool changes refer to changes driven by organizations outside of I2R.

These change scenarios are each described in the sections below. Process flows for each scenario are included in Section 7.6. Process specification details are included in Section 12. The process flows may also be viewed through the master Visio file at: http://workspace/Livelink/livelink.exe?func=ll&objId=18207159&objAction=Open. The native MS Visio process flows may be easier to read and navigate; however, the flows are included here for completeness. Specific detailed flows (e.g., details of the CCB Authorization process) are included in the MS Visio file only.

7.1. Projects

This section describes process variations for IT projects included in Major, Minor, or non-C3 releases.

[7] TestDirector is generally used during projects and releases to capture issues found in testing. However, defects found in the operational systems are occasionally captured there as well; they are supposed to be captured in the I2R Request tool.

Criteria: A project consists of planned system changes that are expected require more than $50K to complete, including development work, QA, and any project management required, and which will be included in a planned releases.

The <company> PLC is the standard lifecycle governing delivery of projects. I2R had previously instituted I2R-specific components into that process (for example, the CCB and the Gatekeeper role). Additional steps and linkages are now added into the new process, such as:

- A Risk Questionnaire that is completed by the requester in the Analysis phase and then revised in the Design phase
- An additional Test Strategy document created by QA in the Analysis phase and formally reviewed by Business, IT, RMO, SIS, and the Risk Analyst
- Formal review forums and approvals for the Test Plans defined in the Design phase (also including Business, IT, RMO, SIS, and the Risk Analyst)
- Linkages between Risk Assessment, ARB, QA, and CCB processes

7.2. Tactical Changes

This section documents the process for smaller changes that will be included in Major, Minor, or Non-C3 releases.

Criteria: Tactical changes are planned system changes that are expected require less than $50K to complete, including development work, QA, and any project management required, and which are bundled into planned releases.

The process for tactical changes is very similar to that for Projects. The key differences are:

- The lead-time is frequently shorter than for projects planned into major releases
- Some deliverables, such as the Test Strategy, are done for the release or the IT track as a whole, rather than for each tactical change
- Other QA documents may still be developed for each tactical change; however, the scale and depth of each may be considerably smaller
- The ARB review process for tactical changes is simplified, with a single ARB review point in the Analysis phase (assuming no major issues or re-work are identified in that review)
- The responsibility for stage approval for tactical changes planned into releases belongs to RMO, as it does for projects

7.3. Proposed Release Exceptions

Changes will generally be directed into planned release windows. Alignment of changes with planned release windows ensures that changes follow a rigorous lifecycle with respect to formal documentation of requirements, functional specifications, testing, user communication, etc. per the <company> PLC.

While changes that occur outside of planned releases will still be expected to meet documentation requirements with respect to change definition, risk assessment, testing performed, and test results, the degree of documentation formality is likely to be less for those changes. For this reason, release delivery is preferred.

The CCB has the authority to designate or reject specific changes as "Release Exceptions", i.e., changes that occur outside of planned release windows. The criteria for release exception consideration are listed below.

Criteria: At least one of the following conditions is met:

- The change is of highest priority and the benefits of the change merit inclusion as soon as possible
- Including the change in a release would extend the release downtime window past an acceptable level
- The change is of high priority, but inclusion in the next possible release has risks due to dependencies on other changes planned in the release

The CCB has full authority to determine whether the criteria met are sufficient to designate the change as a release exception.

Designation as a release exception does not relieve the change team of any obligations with respect to risk assessment and testing. Adequate testing based on risk assessment is still required, and all changes will require pre-deployment gatekeeper review and final CCB approval.

If downtime is required, it is preferred that the release exception be implemented during existing downtime windows, unless there are strong justifications for implementing a change outside those windows.

Process flows are included in Section 7.6. Process details are included in Section 12.

7.4. Emergency Bug Fixes (EBFs)

Emergency Bug Fixes (EBFs) take a special path through the change control process in that they are reviewed post-deployment; they do not require pre-deployment approval.

Criteria: Emergency bug fixes are immediate changes needed to address P1 or P2 Alliance cases for I2R production systems.

Any change that does not meet the criteria shall not be implemented without prior CCB approval.

For I2R-supported applications and infrastructure, CACO drives identification and implementation of needed EBFs. In some cases, CACO may collaborate with other IT organizations, such as Infrastructure IT groups, for implementation.

For non-I2R-controlled tools defined as critical to TS business, the support teams responsible for maintaining those tools shall identify and implement EBFs for those tools. Proposed EBFs for non-I2R tools are required to meet the criteria above to bypass CCB pre-deployment approval.

Change implementers must notify CCB of EBF changes post-deployment, so that the CCB is aware of all changes made to systems within its scope. The requester must send an email to the i2r-ccb alias that contains the CR number, an indication that the CR was implemented as an EBF, and a short description of the reason (e.g., to resolve a particular P1/P2 case).

Change implementers must also notify the gatekeeper of the change within 24 hours by sending an email to the gatekeeper by using the "i2r-gatekeepers-duty@epage.<company>.com" alias. The implementer must provide to the gatekeeper evidence of testing performed. The gatekeeper will follow up 24 hours after deployment of the EBF to verify that the requester has completed both the necessary test cases and the PCC template, and that the request has approval from at least 1 member of the CCB.

The CCB may determine that particular EBFs require ARB review post-deployment. In that case, the change requester will be notified of the decision and will need to schedule ARB review for the change.

7.5. Infrastructure and Non-I2R "Top X' Tool Changes

There is a corporate initiative to improve IT change management practices across <company>. This initiative was too early in its development for this team to implement major changes to the way I2R interacted with Infrastructure IT groups and IT groups managing non-I2R-controlled tools that are critical to the I2R business process (i.e., "Top X" critical systems).

I2R-impacting infrastructure and Top X tools changes were brought into the interim change control process in September 2006. The sole change to that process for the December go-live is the addition of Analysis-phase CCB review for I2R-impacting projects. Formal Risk Assessment for infrastructure and Top X tool changes has been deferred to a future process revision. Improved and earlier engagement with CACO and CA-QA for Infrastructure changes will be achieved in the 1.0 process through Analysis-phase CCB engagement and the CACO and CA-QA participation in that forum.

Some ideas for how the I2R CCB could interact with a centralized CCB, when instituted, were captured in a separate document[8]. The Operational Excellence

[8] http://workspace/Livelink/livelink.exe?func=ll&objId=18641770&objAction=Open

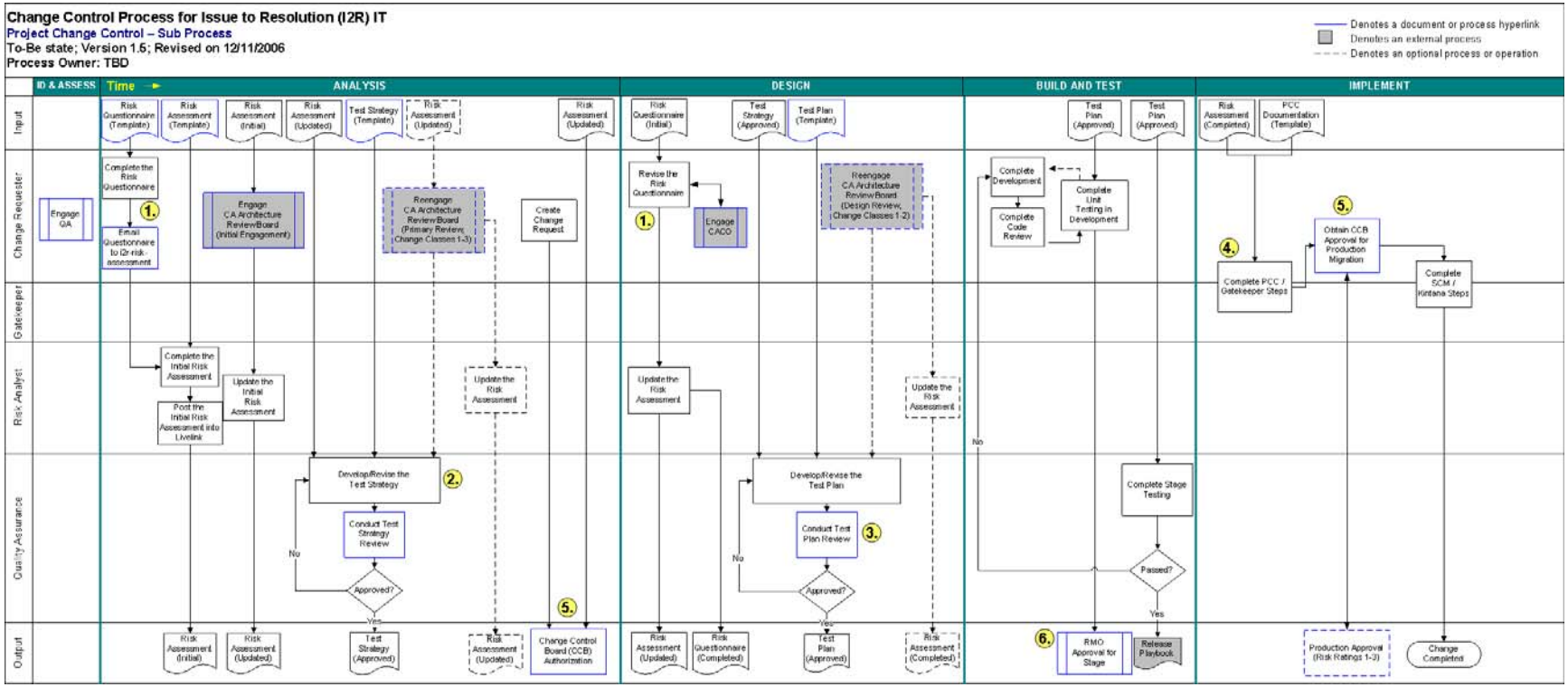
organization will have the responsibility for defining the interaction of I2R change control with corporate-level IT change control

Although no formal change risk assessment will be conducted for Infrastructure and non-I2R “Top X” tool changes, the CCB may request answers to questions such as the following:

- Why is this change being done?
- What is the value of the change?
- What specifically will be changed?
- Has a change like it been performed before?
- Do you have a standard process for implementing this type of change?
- Can it be backed out?
- How will you verify that it worked?
- How will you verify that it did not break or adversely impact applications that depend on it?
- How will you proceed if it is determined that the change did cause an adverse impact?

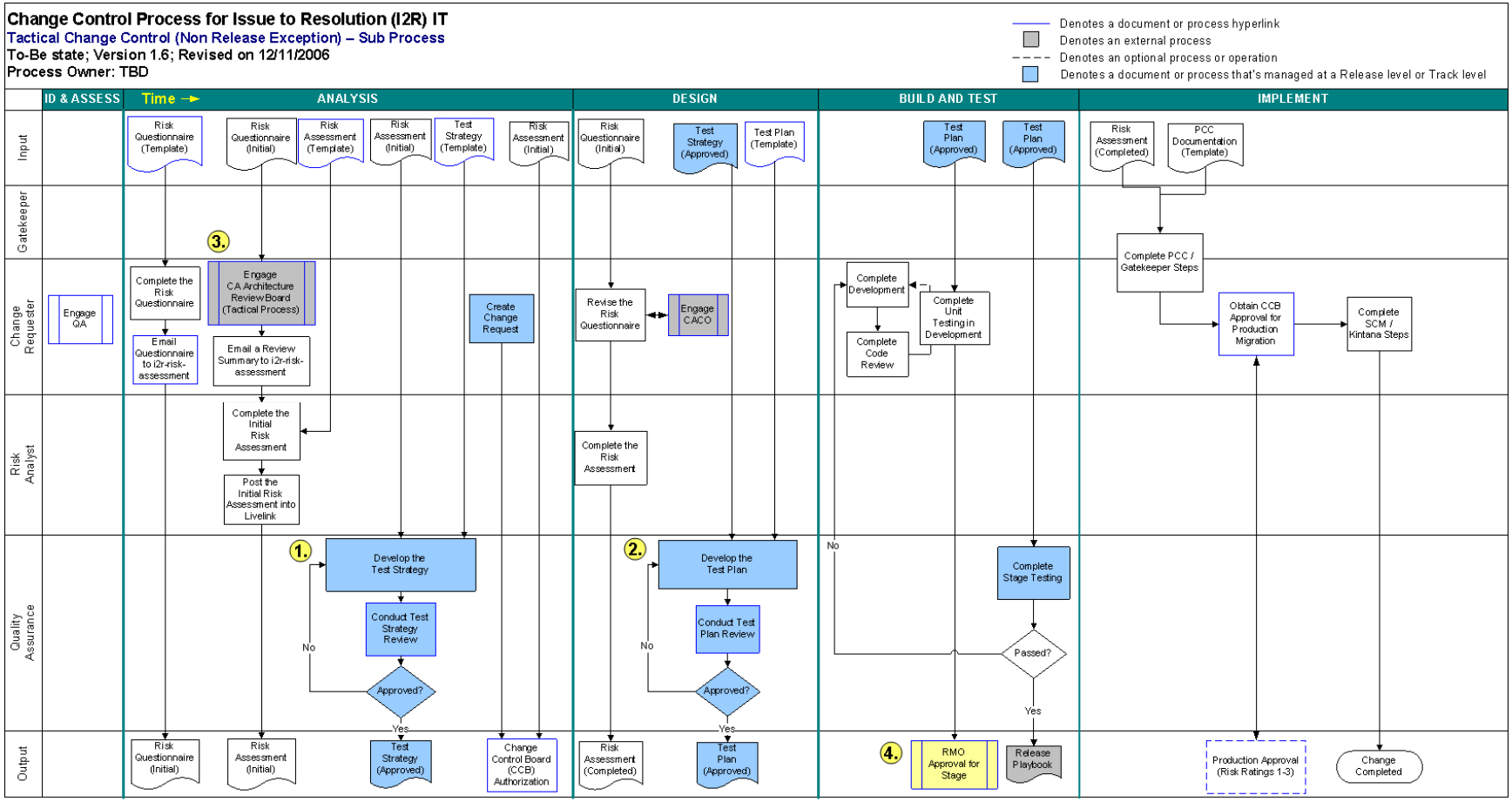
7.6. Scenario-specific Process Flows

Change Control Process for Projects



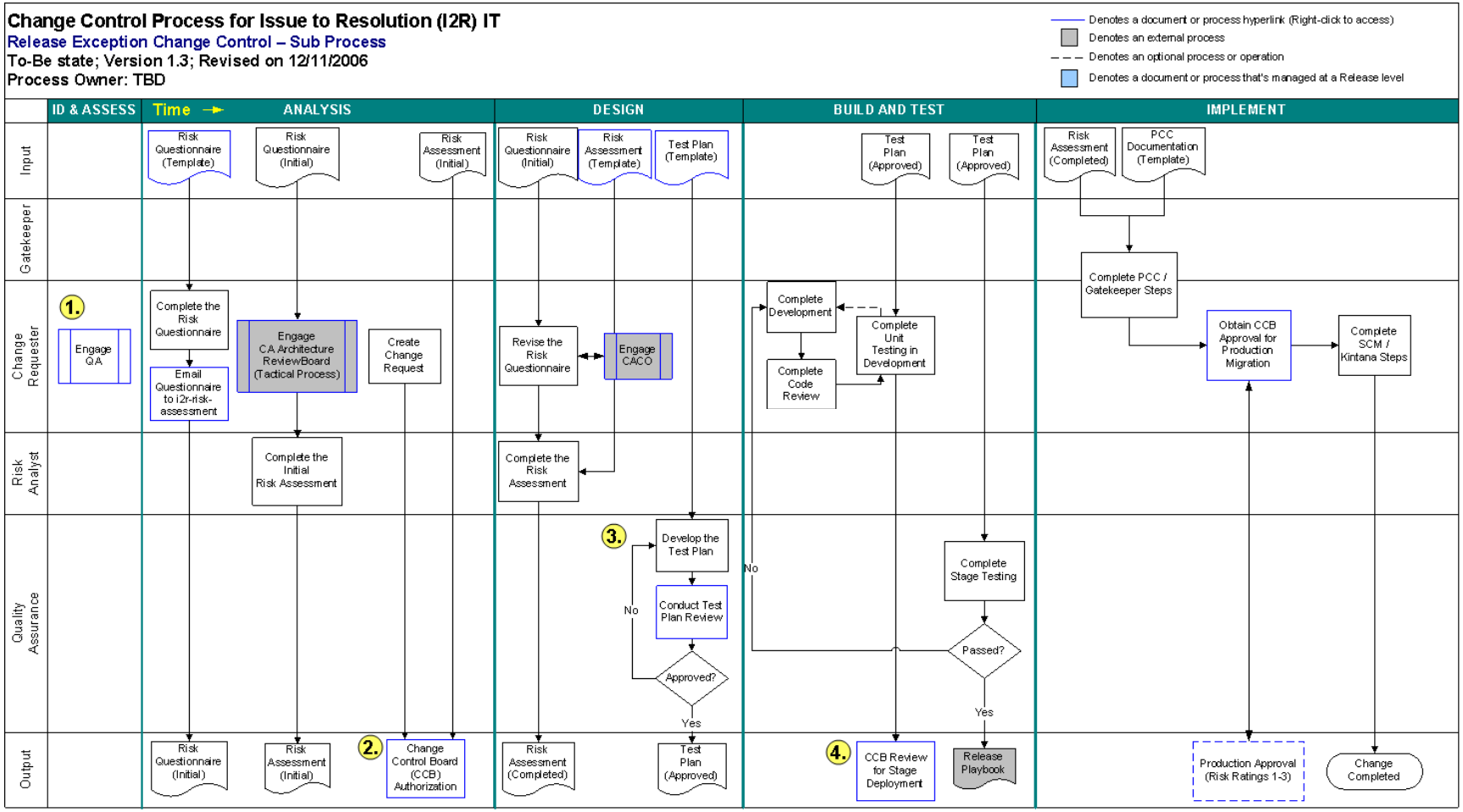
1. The Risk Questionnaire is completed by the Change Requester initially during the Analysis phase and then revised during the Design phase
2. The Test Strategy document is a new deliverable by CA-QA that defines the high-level strategy to verify that the changes function as expected and do not negatively affect other functionality. The Test Strategy uses information from the Risk Assessment, supplemented by the ARB review if conducted, to identify areas of greatest risk and impact, and therefore, test mitigation approaches required
3. Test Plans now have formal review forums, as well as a list of required approvers
4. The Gatekeeper process pre-deployment ensures needed testing was performed to acceptance criteria and is used as the input to CCB
5. CCB authorization and approval has been linked to the risk assessment framework
6. RMO now performs the stage migration approval for planned releases (including projects and tactical changes within them)

Change Control for Tactical Changes



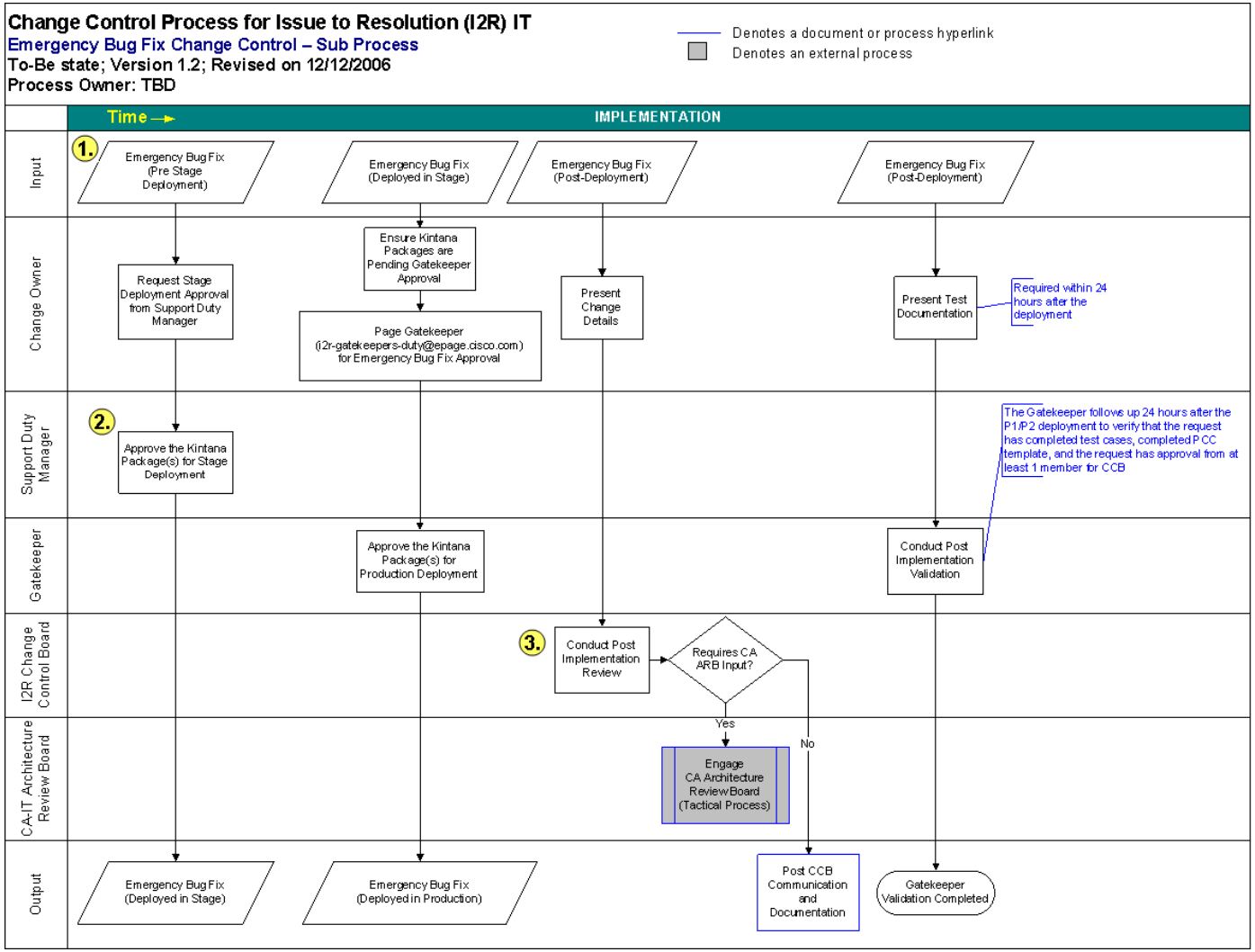
1. The Test Strategy document is developed for the release (major, minor, non-C3) that the tactical changes will be bundled into
2. The Test Plan is a scaled down version using the standard Test Plan template and is completed at the IT track level
3. The ARB review follows the ARB Tactical Process
4. RMO approves the stage migration, as they do for migrations of Projects within releases

Change Control for Release Exceptions



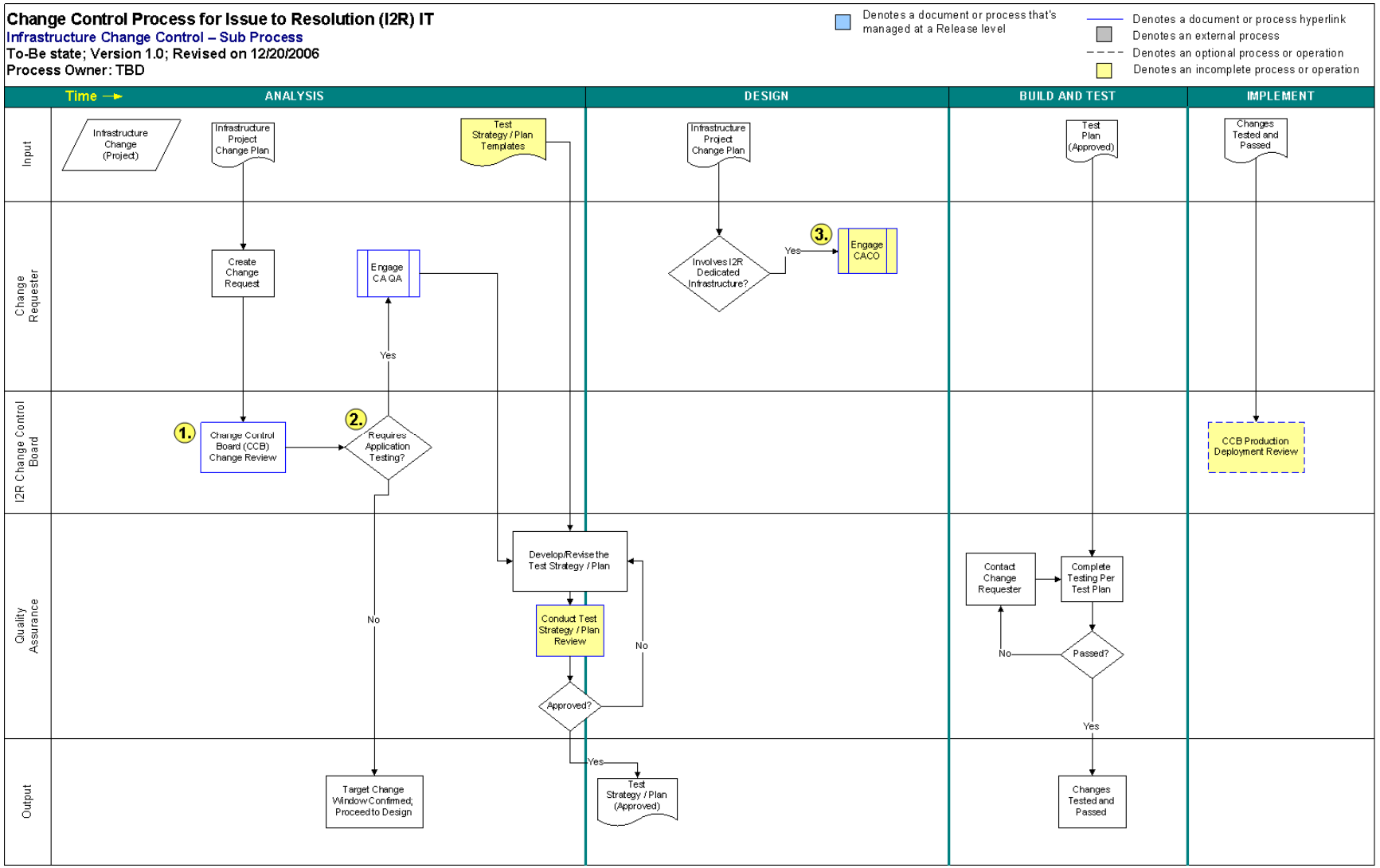
1. QA is not involved in 100% of release exceptions today but is expected to converge toward 100%
2. CCB authorizes (or rejects) a change as a Release Exception at the CCB Authorization step
3. No Test Strategy document is created; a smaller-scale (depending on size of the change) Test Plan *is* created
4. CCB is responsible for Stage approval for Release Exceptions

Change Control for Emergency Bug Fixes (EBFs)



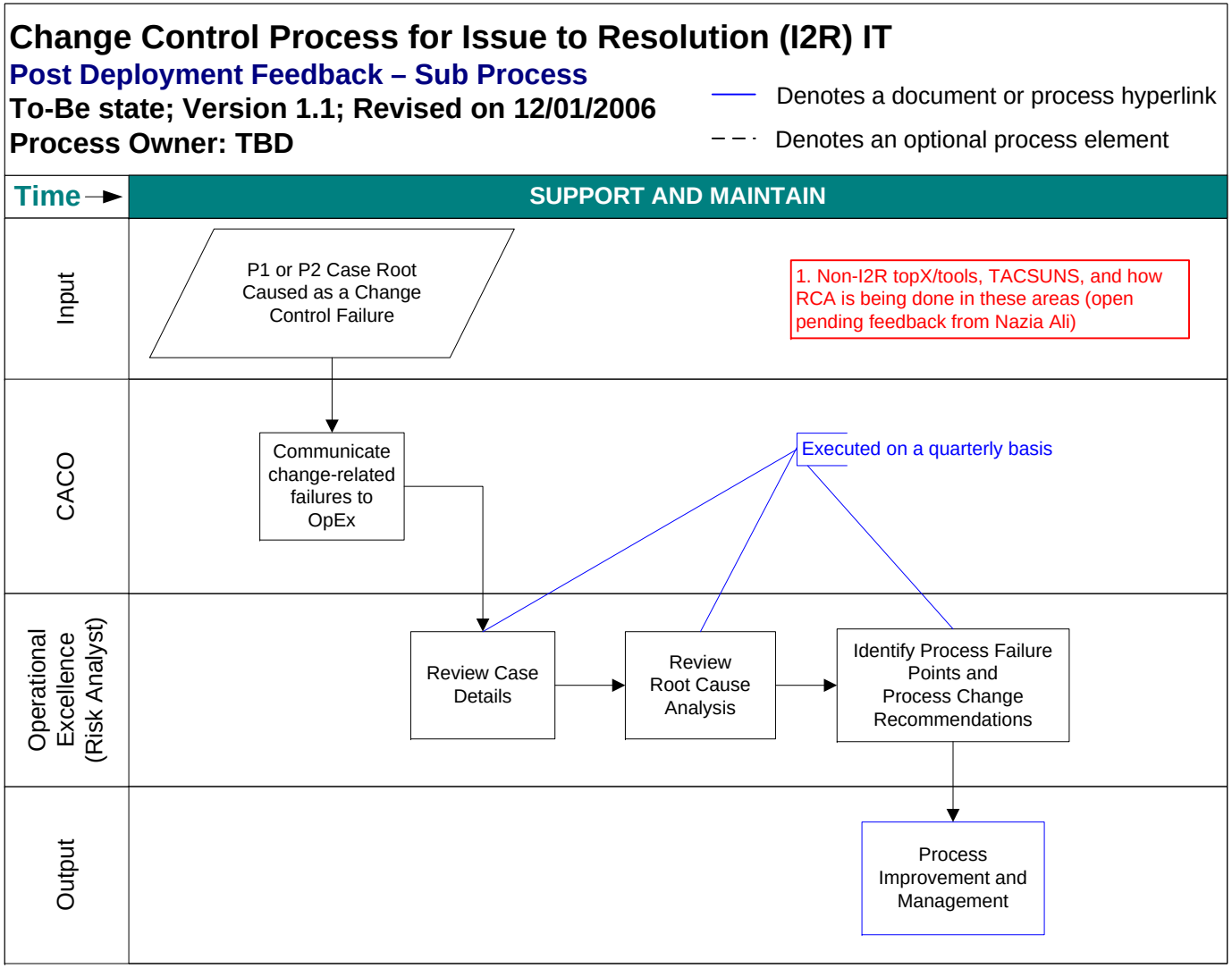
1. Changes routed through the Emergency Bug Fix process must meet the pre-defined criteria for an EBF
2. No CCB pre-deployment authorization is required
3. Change implementers must notify CCB after change deploy to maintain CCB's visibility into all changes

Change Control for Infrastructure Changes



1. Analysis Phase engagement with CCB is requested
2. CCB may determine that I2R functional/application testing is warranted, and may request QA engagement
3. If critical infrastructure for I2R is involved (e.g., amps or ohms servers), CCB may request early CACO engagement to provide visibility into upcoming change

Post-Deployment Feedback



8. Revised Change Control Board (CCB)

The Change Control Board (CCB) began as a change review body for the C3 Oracle 11i system. Over the course of the Tiger Team efforts, it has broadened its scope to all I2R systems, and critical non-I2R TS-impacting tools. The post-Tiger Team iteration of the CCB is described in this section.

8.1. Charter and objectives

The CCB is chartered with ensuring that changes to I2R-impacting systems are properly controlled to minimize negative impact to the business.

Specific objectives:

- Define appropriate change windows for planned changes
- Define appropriate level of change control governance for planned changes
- Ensure planned changes are on a path toward adequate quality assessment (architecture review performed, risks and impacts understood, test strategy defined and agreed, etc.)
- Ensure changes in queue for production deployment have been adequately assessed as to quality and risk and are deemed, given everything that is known about test results and the ability to back out the change if needed, to still have benefits that outweigh the risks of the change

8.2. Scope

CCB reviews changes for all include all I2R-owned applications, infrastructure that impacts those applications, and critical TS/I2R tools outside of direct I2R control. Non-EBF (Emergency Bug Fix) changes shall not be deployed to stage or production environments without CCB approval[9].

The CCB does not perform business prioritization. It is assumed that changes for which the business has allocated funding have been prioritized. However, the risk assessment process does measure the level of risk of a change compared to its perceived benefit. The CCB may reject or redirect planned changes for which the level of risk outweighs the benefit.

The level of CCB change control across the tools within its scope is described below.

Category	Managed By	CCB Role
I2R applications (C3, non-C3)	I2R-IT	Authorize and approve changes

[9] For releases, RMO manages approval for stage deployment (CCB approves release exceptions for stage deployment)

Category	Managed By	CCB Role
Infrastructure underlying I2R applications (databases, servers, etc.)	Infrastructure IT	Authorize and approve changes
Infrastructure impacting TS (e.g., core services)	Infrastructure IT	Identify possible negative impacts (e.g., deployment windows during key business hours, etc.), as well as needed actions to address the issues
Non-I2R critical tools for TS	Various non-CA IT groups	Identify possible negative impacts (e.g., deployment windows during key business hours, etc.), as well as needed actions to address the issues

The CCB does not replace any gates dictated by the <company> PLC. However, **Execute Commit (EC) is not valid for TS/I2R IT projects without prior CCB approval**.

CACO P1/P2 Emergency Bug Fixes (EBFs) will be reviewed by CCB post-deployment, in order to provide visibility to the changes made. No prior CCB authorization or approval is needed to deploy an EBF. Criteria for what defines an EBF versus a change that can wait are listed in Section 7.4.

CCB authorization is needed at the following timings:

- TS/I2R Projects in Analysis phase (pre Execute Commit)
- TS/I2R Enhancement/tactical releases (pre Release Commit)
- Boundary and Critical applications and Infrastructure projects (prior to EC)

CCB pre-stage deployment approval is needed for the following:

- TS/I2R Release exceptions
    - Note that RMO owns responsibility for stage approval and migration for planned releases (major and minor, C3 and non-C3)

CCB pre-production deployment approval is required for the following:

- Any non-EBF production deployments (post readiness review)
    - For planned releases, this review will occur post-readiness review. For efficiency reasons, the CCB may opt to attend readiness review and make the decision in that forum
    - For release exceptions, CCB production approval review will occur after the gatekeeper review and prior to production deployment
    - For Boundary and Critical applications and Infrastructure projects, CCB approval review will occur prior to production deployment

8.3. Membership

The CCB membership for the revised board is shown in the table below.

Voting Members	Non-Voting Members
CACO	Facilitator
TS/I2R Business	Release manager C3
CA IT delivery	Release manager non-C3
CA QA	Infrastructure[10]
	Change Requesters (mandatory)
	Risk Analyst[11]

In addition, there are identified subject matter experts (SMEs) for the following subject matter areas that are available to review requests offline:

- TACSUNS
- ACS
- GSSC
- TAC/CIN
- SWC
- Entitlement
- Reporting
- SSM

8.4. Logistics

CCB meetings are conducted Mondays through Thursdays at 1pm PST for 60 minutes. There are no scheduled CCB meetings on Fridays, as it is too late for weekend deployments. Extended meetings may be arranged to review releases.

Participants include the voting and non-voting members listed above. In some cases, specific subject matter experts may be asked to attend.

All voting members must be present to constitute a quorum. In specific situations, the meeting may proceed with three voting members, as long as the fourth member is including in the voting prior to decision finalization. All voting members must signoff on *all* changes. Each member shall have a designee when the member cannot make the meeting (e.g., due to PTO). In that case, the designee shall be given decision authority on behalf of the absent voting member.

The CCB agenda is controlled by a facilitator. To put a proposed change on the agenda, requesters contact the facilitator through the i2r-ccb alias. These email requests must be received by noon PST on the day prior to the CCB meeting. The request must contain a reference to the Change Request (CR, I2R, Empower, TD).

[10] Infrastructure CCB membership to be re-evaluated in 2-3 weeks after launch
[11] Risk Analyst CCB membership to be re-evaluated in 2-3 weeks after launch

The facilitator assembles all Change Requests to be reviewed for a particular day into a report that is used to guide the meeting and capture meeting decisions and next steps. The meeting agenda is sent out end of day the day prior to the meeting.

CCB voting board members are expected to review the change requests and their associated risk assessments prior to the 1pm CCB review meeting.

The CCB does not perform business prioritization. Changes going before CCB are presumed to have been high enough priority to have been assigned the requisite resources. However, part of the risk profiling and assessment measures the degree of change risk compared to change benefit. The CCB may use that information to identify whether a change should proceed. For example, a change perceived to be high-risk and low-benefit may be redirected or delayed.

Decisions are communicated to stakeholders following the meeting, using the alias i2r-ccb-comms.

CCB decisions may be appealed to the I2R Delivery Leadership Team decision body for further consideration. (Note: Given increasing amounts of SSM functionality within C3, SSM representation may need to be added.)

9. Tools

9.1. Kintana

Kintana is used to migrate source code into Stage and Production environments. At the time of this initiative, most (but not all) I2R systems used Kintana to migrate source code. At the time of this report, around 120 of the applications listed in the application repository use Kintana for source code migration[12].

Kintana is workflow-oriented with defined approvers for each migration setup. This project focused on the approval steps to push to the Stage environment(s) and to Production. At the outset of this program, the approvers for those migrations were in some cases the developers implementing the change, so that no real change control was in place for many I2R applications.

There is no standard source code migration workflow for I2R-IT, and the existing workflows used are not consistent across applications. Each workflow has different steps to completion. The two most common workflow types used for I2R are "ERP11i" (used for C3 deployments) and "Deploy2" (used by a large number of non-C3 applications). (The others include "cco", "google-topic", and "onesizefitsall".)

The ERP11i workflow has a single set of approvers; Deploy2 has a separate set of approvers for each application. The ERP11i workflow has two sub-flows: one to deploy to stage and production; the other to deploy to the business layer environment. The approvers for both sub-flows are the same.

The two key gaps to address with respect to Kintana change control are:

- Modifying the approvers for stage and production migration steps for I2R applications to correspond to the appropriate approval bodies in the revised change control process
- Modifying the list of "root approvers" (the roles with the authority to manage the approval lists for the workflows) to limit the approved approvers to specific change control process team members (at this time identified as Sherman Chiu, May Tran, and Danny Liu)

9.1.1. Work Completed During Tiger Team Existence

The following tasks were performed within the context of this project:

- Audited all Kintana workflows using the application repository as a reference
- Identified, for all I2R applications using Kintana, the workflow was used by each, the type of workflow, the existing root approvers were
- Identified specific changes to make to the workflow approvers and approver list management (using the root approvers)

[12] Not all tools are listed in the application repository. Known gaps include all TACSUNS tools and the non-C3 PSIRT tool deployed in early 2006 and not yet transitioned to CACO.

- Changed root approvers for the stage and production deployment approval steps (K3 and K5) to identified Change Control process team members (implemented November 27)

9.1.2. Next Steps and Ongoing Work

The following tasks remain:

- Go through each workflow's set of approvers, define the right approver list, correct the approvers for each
- Communicate to the new approvers that they will be expected to do the approval into stage or production
- Remove the old approvers

The new approvers will be:

- K3 gate (push to Stage): RMO for releases; CCB for release exceptions
- K5 gate (push to Production): QA gatekeeper. Subsequent to OnePCC rollout, IT-PMs will be allowed to approve deployments as the CCB approval will be managed in ITG and linked to the Kintana process.

The Deploy2 workflow will take the most work to address, since each application has a distinct set of approvers.

Ongoing team members will include May Tran and Zach May, with some participation on the part of Sherman Chiu and Danny Liu.

The OnePCC deployment will use the same instance of Kintana as is used by I2R currently, so that the changes mentioned above are in support of a more fully tool-enabled change control process currently targeted for March 2007.

9.2. OnePCC Planned System Rollout

OnePCC is a <company>-wide initiative to implement improved change control tool capabilities to better support Sarbanes-Oxley (SOX) compliance. The OnePCC implementation is a mandated roll-out, with targeted deployment in Q307.

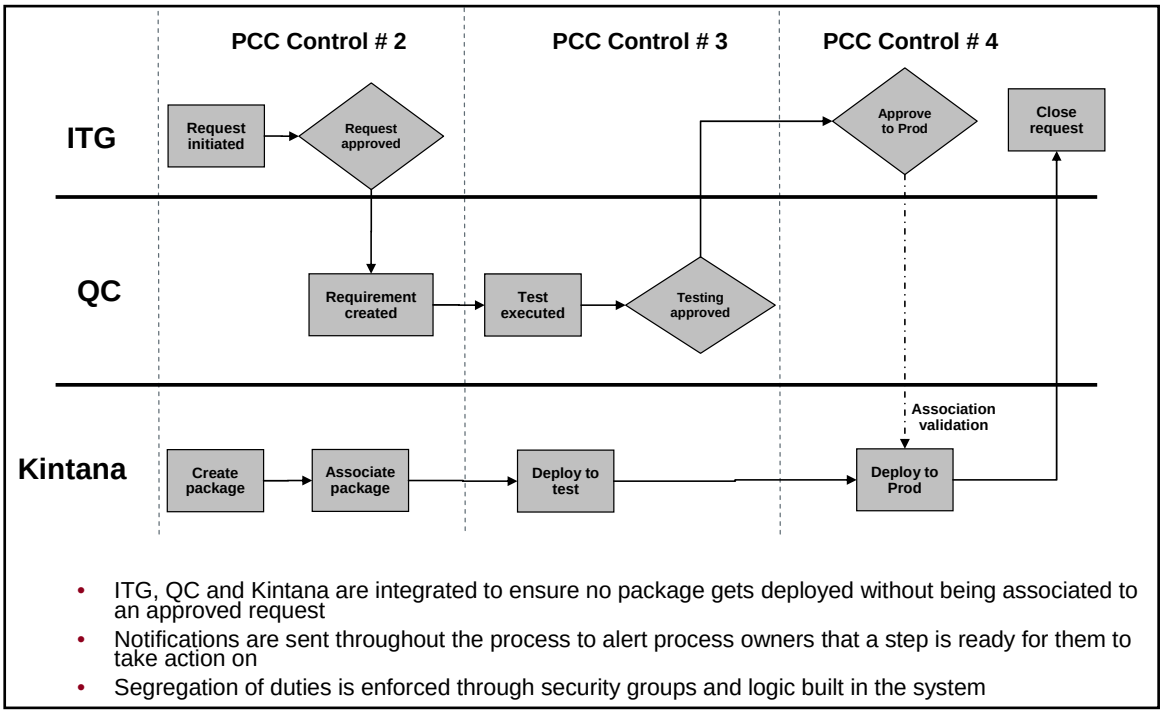
The objectives of the OnePCC deployment are to:

- Provide a solution that can enforce change controls and facilitate compliance
- Drive standardization of process and use of tools already in-house
- Consolidate evidence for Program Change Control (PCC) application testing
- Reduce the dependency on application owners for gathering change evidence
- Provide read-only and report access to allow auditors to review changes and control evidence

The planned OnePCC solution integrates Kintana, a change request tool (ITG)[13], and a test tracking tool (Quality Center). Descriptions of the scope of each of these tools and their interactions are provided in the table below:

Tool	Scope
ITG	Capture and manage change requests, including change approval and approval for production migration
Quality Center (QC)	Manage requirements, test cases, and test execution results; provide test results to ITG to facilitate production deployment approval
Kintana	Migrate source code to stage and production environments; ensure production migrations are approved through interface with ITG

The planned OnePCC process flow for projects and bug fixes is shown below.



- ITG, QC and Kintana are integrated to ensure no package gets deployed without being associated to an approved request
- Notifications are sent throughout the process to alert process owners that a step is ready for them to take action on
- Segregation of duties is enforced through security groups and logic built in the system

ITG and QC security group configuration will be identified in December. Detailed training started November 20, 2006. The I2R ongoing change management team will be participating in the training.

OnePCC implementation for I2R will require some I2R resources to support the 2007 deployment. The OnePCC organization adoption responsibilities for I2R have not

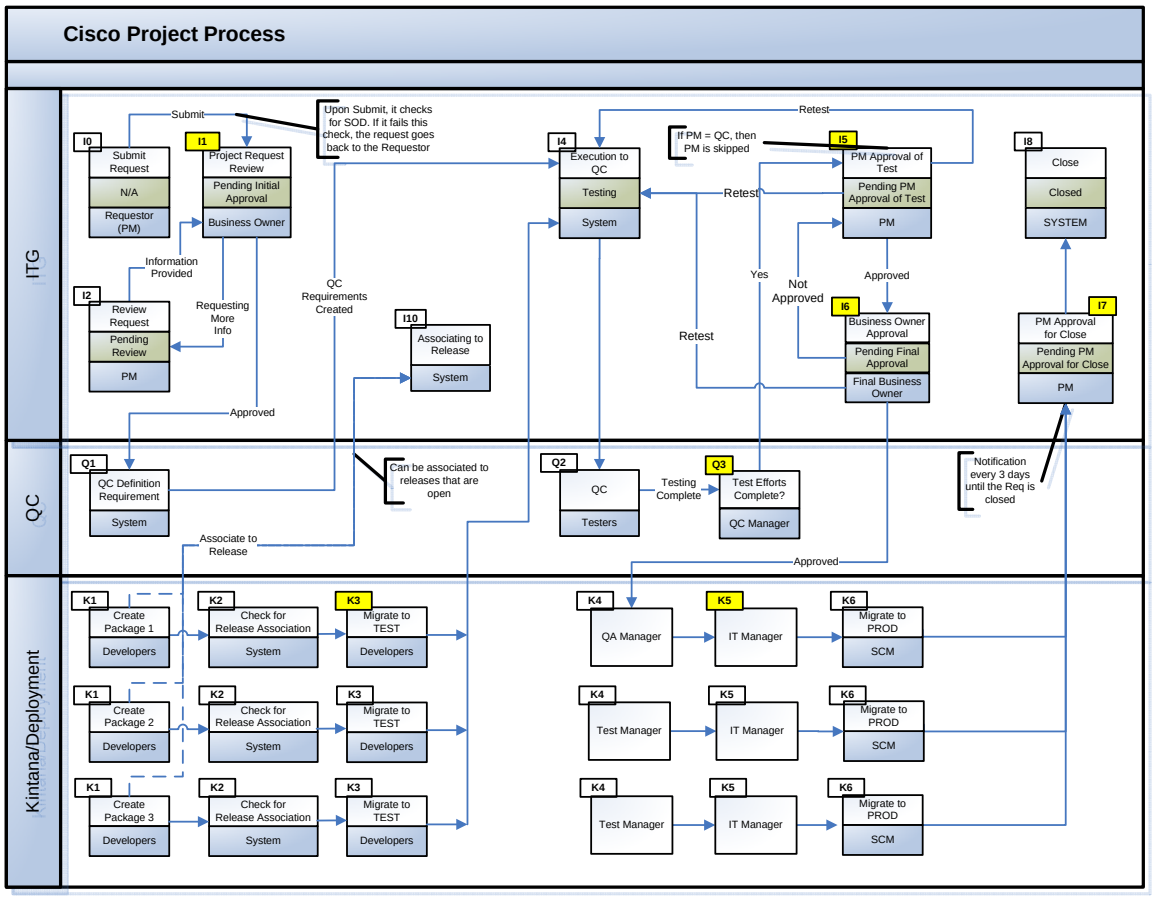
[13] The current change request tool for projects, EmPower, is a highly-customized version of ITG. The OnePCC deployment will be a configured, but not customized, implementation.

been defined at this time; however, the team may consist of: May Tran, Danny Liu, and Sherman Chiu.

The OnePCC Implementation Timeline is under review at this time. As of mid-November, the dates were as listed below; however, the deployment date moved from February to "somewhere in Q3". Final dates are TBD. Preliminary dates were:

- December 2006: Training and application configuration
- January 2007: Integration, System, and User Acceptance Testing
- Mid-March, 2007 (post March release): Go-live for C3 (non-C3 is TBD)

OnePCC has seven main approval gates, shown in yellow in the figure below[14].



The approval gates and their meaning are described below:

[14] The flow shown in the diagram is for Projects. Bug Fixes and Emergency Bug Fixes are in separate flows. All flows can be found in the OnePCC folder on LiveLink: http://workspace/Livelink/livelink.exe?func=ll&objId=18399094&objAction=browse&sort=name

Gate	Tool	Authority	Approval Meaning
I1	ITG	CCB	The proposed change has been approved
K3	Kintana	RMO/CCB	The change is ready to be tested in the Stage environment
Q3	QC	Gatekeeper	The change has been tested and has met readiness and acceptance criteria
I5	ITG	IT PM or business owner	The business has agreed that the change meets readiness and acceptance criteria
I6	ITG	CCB	The change control authority approves the change deployment into the Production environment
K5	Kintana	IT PM	The change is approved for Production migration (note that K5 will be owned by the Gatekeeper until OnePCC deployment)
I7	ITG	IT PM or business owner	The change has been deployed and can be closed out

The March deployment will cover the ERP11i Kintana workflow for the C3 and related applications. Non-C3 deployment will occur subsequently; target timeframe is not currently known.

Neither deployment is targeted to cover TACSUNS applications, as they do not use Kintana at this time.

For more information on the OnePCC, refer to the following Livelink folder: http://workspace/Livelink/livelink.exe?func=ll&objId=18399094&objAction=browse&sort=name. May Tran is the I2R contact for OnePCC.

9.3. Automated Dependency Mapping Pilots

Dependencies between applications are currently managed using <company>'s EMAN tool. Each application's dependency list is manually maintained. The dependencies are used to identify affected or potentially affected resources due to a Change Request (CR). In addition, EMAN-generated system outage cases are prevented during a planned downtime window to an application and its dependencies.

Numerous failures have occurred due to unknown or undocumented EMAN dependencies. Alliance cases may result when a dependency is not documented. In addition, any teams using the dependency information to guide test approach or coverage may miss testing critical areas, particularly boundary systems, when implementing changes to systems. Unanticipated impacts were, for I2R, one of the most significant causes of P1/P2 cases.

The Excellence in Operations (EiO) organization conducted two pilots in summer/fall 2006. Key learnings and conclusions are documented below. The presentations from the proof-of-concept readout meetings can be found at the link below:

http://workspace/Livelink/livelink.exe?func=ll&objId=18644407&objAction=browse&sort=name

9.3.1. Magnum Technologies

Magnum Technologies has a suite of tools/applications related to business impact management, application monitoring, and service level management. It has the capability to replace a broader set of EMAN features beyond just dependency management. However, it appears to be a fairly complex suite of tools; implementation would require creation of an Alliance interface, replacement of some portions of EMAN functionality, integration with other portions, etc. The ability to easily implement specific areas of functionality only was not clear from the demonstration.

Some features noted in the proof-of-concept readout:

- Ability to comprehend redundancy of systems, for example to identify whether an outage of a component results in an outage to the user, and to reflect outages only when the system is actually down to the user (while raising alerts to IT whenever specific redundant components go down)
- Ability to define KPIs to support reporting how well an asset is supporting a business function
- Ability to discover unknown linkages between systems by monitoring communications among applications and components
- The vendor described the system as “open architecture” – it was not clear how easy it would be to use some components while interfacing others, nor how easy it would be to not implement specific areas of the application that are less critical to I2R’s and <company>’s current issues
- The vendor indicated that it could leverage existing EMAN functionality; implementation complexity was not clear

Summary

Manual (and insufficient) dependency management is a key stability issue today. An automated tool to address that gap would be valuable to IT teams across <company>. In the longer term, application monitoring that reflects the business experience would be a next-level best-practice improvement – and would support better service level management between IT and the business and between dependent IT organizations.

EMAN has application monitoring capabilities today beyond those typically used by I2R applications, for example the ability to implement site-specific monitors to capture performance experienced by users across sites. The choice to address performance monitoring by implementing a standard tool or by auditing and

improving use of EMAN capabilities for <company>'s most critical tools is a strategic one.

An implementation of this tool would be complex and fairly large and would make most sense as a corporate-wide initiative with staged rollouts. It does not appear to make sense for CA or I2R to invest independently in a tool of this scale.

The EMAN suite of tools has been built over a significant period of time and its replacement or partial replacement by a standard off-the-shelf package would be an extensive implementation.

It is unclear whether the EiO organization will be making a recommendation based on this pilot or will depend on individual IT organizations to make their own decisions. In addition, the relevant central IT initiatives (Change Management, Performance Management) may or may not propose a direction.

9.3.2. Mercury Interactive

The Mercury Interactive read-out deferred to December 1st. Due to time constraints, the team elected not to include a formal summary of that readout in this report. The Infrastructure-driven Change Management track owns the responsibility for identifying tools needed to support improved change management at <company>. The responsible individuals should be contacted to obtain conclusions from that pilot. CA's Operational Excellence team properly owns the responsibility from a CA perspective to ensure tools enablement decisions within that track are consistent with CA needs.

10. Metrics

Key metrics are listed in the section below. A minimum set is proposed for the immediate-term, until there is an organization in place with responsibility for calculating the metrics on a periodic basis and monitoring and reporting results. Near-term metrics are proposed in the next two sub-sections; suggestions for additional future measurements follow in the third sub-section.

10.1. Process Adoption Metrics

Process adoption metrics measure the conformance of an organization to specified processes. The intent of measuring process adoption is to evaluate the degree to which new processes have been adopted; adoption shortfalls may then be addressed through additional training, communication, incentives, etc.

The following metrics would provide reasonable visibility to management (e.g., TS DLT) as to the degree of conformance to the change control processes.

Metrics below are recommended to be calculated and reported quarterly.

Metric	Method	Target
Percent of changes for which a risk assessment has been completed	Captured during CCB review discussions for each change on the agenda; reported by change category (project, tactical, release exception)	100% by Mar 07
Percent of changes using CA-QA for testing	Calculated by risk analyst using questionnaire; reported by change category	Projects: 100% now; Tacticals: 100% by Mar 07 Release exceptions: TBD
Number of projects, minor releases with approved Test Strategy, Plan	Number of projects with the required sign-offs for those documents Number of minor releases with required sign-offs for Strategy Number of tacticals with associated Test Plans	Projects: 100% in CY07 Minor releases: 100% in CY07 Tacticals: TBD

10.2. Results-oriented Metrics

Metrics below are recommended to be calculated and reported quarterly.

Metric	Method	Target
Change-related cases per month	Reported by category (application, infrastructure, TopX, TACSUNS) using Health Reports	TBD (baseline is 4/mo)
Key cause areas	Cause attribution using health reports and case notes into key process cause areas (test planning, impact assessment, etc.)	N/A

10.3. Informational (Future) Metrics

A few other useful metrics are listed in the table below. Until a formal organization is in place with responsibilities to measure and monitor the results, a minimum-set list should be established.

Metric	Method	Target
Reason for change (user request, enhancement, fixes, etc.)	Captured from change request tool(s). Ideally suited for when a single request tool (ITG) is in use.	N/A
Percent of changes that were backed out	Captured from change request tool(s). Ideally suited for when a single request tool (ITG) is in use.	N/A
Percent of changes that occurred outside of a release	Captured from CCB review	TBD
Number of changes rejected (with categorized reasons)	Captured from change request tool(s). Ideally suited for when a single request tool (ITG) is in use.	N/A
Number of times an application has been changed	Captured from CCB change review data or from change request tool	N/A
Number of emergency changes (with reason codes)	Captured from CCB change review data or from change request tool	N/A
Change area (application, infrastructure, non-I2R tool)	Captured from CCB review	N/A
Number of changes within a release (# projects, #tacticals)	Captured from CCB review for the release	N/A

11. Next Steps for Change Management

This section describes findings (new issues or outstanding issues not addressed by the team), recommendations, next steps, and lessons learned over the course of the project.

11.1. Findings

Deployment date for the revised Change Control process is scheduled for December 2006, subsequent to the completion of this document. Process adoption and outcome metrics should be collected after the new process is instituted to measure the results of the revised process and identify further needed improvements. Findings in this document are based on known failure areas and gaps identified during the process definition work. The Change Control process team owns the action to measure outcomes for the new process until the Operational Excellence team is established and takes ownership.

Findings were noted along the following dimensions:

- Infrastructure change management
- QA processes and coverage
- Documentation
- Prioritization processes
- Process evolution and improvement

11.1.1. Infrastructure Change Management

Interim change control measures significantly reduced change-related failures. Of the remaining change-related cases, 69% in Q107 of them were due to changes to infrastructure components upon which I2R systems are dependent. More than half of those cases were due to configuration errors introduced when performing system changes; in some cases, it was not known how particular configuration settings “became wrong”. In other cases, planned changes were implemented incorrectly. There is a significant opportunity to reduce the number of these cases through better infrastructure change management practices.

11.1.2. QA Processes and Coverage

The Gatekeeper role performed by QA has resulted in a reduced number of change-related cases; however, there have been known failures. Detailed analysis of the failure causes has not been performed. Anecdotal data suggests that some changes may have bypassed the Gatekeeper process, and that some issues may not have been caught within the process that should have been. The Gatekeeper role itself transitioned several times over the course of the project; failures may have been due to failures in the transition or in the activities of specific individuals performing the role during specific periods.

As of Q107 (August 2006), CA-QA was targeted to cover 100% of application changes pertaining to I2R systems. For formal IT projects, the adoption rate does

appear to be high. However, QA does not have 100% coverage for tacticals and release exceptions. QA is involved in about 25% of tactical changes[15]; developers (IT/CACO) are performing testing in other cases. QA is not officially involved in minor releases, except for any tacticals or projects within those that have QA planned. Release exceptions do not appear to have QA coverage. Coverage for C3 tacticals appears to be higher than for non-C3 tacticals. This issue was raised at the November 16th Delivery Leadership Team (DLT) meeting; the DLT confirmed that 100% QA coverage was still the expectation. Multiple action items are being tracked at the DLT to close this issue[16].

Stakeholders have identified other gaps in QA processes over the course of the project, generally during release-oriented discussions. Key concerns included: lack of visibility into what QA would test and how, including lack of formal group review and approval to ensure coverage would be adequate; and ongoing issues with knowledge transfer into and retention by QA. The team has attempted to solve the first issue by adding the Test Strategy document and formalizing the review and approval process for the existing Test Plan document. The knowledge transfer and retention issue remains open and is a difficult to solve, given that QA is largely outsourced and the vendor appears to have significant turnover.

11.1.3. Documentation

Lack of documentation describing systems and their interactions was noted as a significant gap at the time of the original case analysis. A few architectural documents have emerged since that time, but documentation is still very limited. The I2R systems environment is extremely complex, with more than 120 different systems in use; very few people understand how the systems interact. Lack of architectural documentation significantly hinders the ability to identify possible impacts of changes, which means that possible impact areas may not be tested, and stability issues may still be introduced due to change activity. The increased level of control over changes has helped decrease change-related stability issues, and formalized risk assessment will contribute as well; however, lack of adequate documentation may still result in unanticipated negative impacts from change.

11.1.4. Prioritization Processes

Prioritization of IT projects is not strictly speaking a change control issue. However, it did arise as a gap many times over the course of the project as issues arose and resource decisions needed to be made. There appears to be no formal decision-making process or prioritization structure to enable resource and budget trade-offs and allocations within IT.

Some IT work has defined priority levels. For example, IT projects tied to initiatives (CA, TS, or BPOC) are considered high priority. Small “tactical” changes have priority and severity levels available as selections in the I2R request tool; these values *are* used. Larger IT work – projects, or “CFPs” that are not tied to initiatives have no clearly articulated priority level. Any IT project work that

[15] Information provided by CA-QA organization
[16] The DLT contact is Dennis Jaramillo

the business opts to fund is added to the IT roadmap, regardless of the degree of other changes going on in parallel and ability of scarce resources to support it. As a result, if there are resource or budget (or system environment) conflicts that arise later, there is no decision-making structure to support making trade-offs.

Some examples of issues over the course of the project: recurring issues in determining how to fill resource gaps when project resources became unavailable (consultants let go; internal resources moved to other projects); determining how to address budget shortfalls in QA costs; determining how to address IT track resource needs to support the work of the Performance team, etc. Each resource and budget issue encountered was painful and complex to resolve – the process generally amounted to gathering the IT managers in a meeting and seeing who would volunteer to give up money or people.

Despite extensive use of outsourced resources, IT work remains highly dependent on scarce internal resources, such as IT track subject matter experts, QA internal resources, CACO internal resources. CA does not have unlimited bandwidth to implement change. IT implementation results (time, predictability, quality) may be improved by prioritizing all IT work that CA does, and choosing to implement fewer, higher priority changes.

11.1.5. Process Evolution and Improvement

The findings in this section related to natural evolution of the Change Control process as outcomes are measured and further improvements are made.

There are some overlaps in the content of the risk questionnaire, ARB questionnaires, and the SOX/PCC questionnaire. We were not able to fully streamline the interaction of these three processes within the time frame for this project.

In addition, although we proposed getting rid of the Impact Assessment Document (IAD), a few individuals do use this document currently. We have not identified any downstream consumers of the content, however, and the IAD is not widely used.

The Risk Assessment framework will require tuning (criteria, weights) over time as experience with the framework is developed and new information gathered.

11.2. Recommendations

The following recommendations are in priority order.

1. **Recommendation:** *Collaborate with infrastructure IT teams to address infrastructure change management issues.*

   Priority: High

   Owner: Operational Excellence

   Key Organizations and Roles: CACO, Infrastructure, CSR Change Management team

Infrastructure change management practices have significant gaps that affect CA and other <company> organizations on a daily basis. The continuing activities from the Case management team include defining operating level agreements (OLAs) with IT support groups. Those OLAs should include change management guidelines that define expectations for changes to I2R-impacting infrastructure. Suggested guidelines to address known infrastructure change issues:

- *Any* change to a system (reboot, configuration change, killing a locked session, new hardware added, etc.) shall require two individuals to implement (and plan) the change to reduce the likelihood of mistakes
- *Any* change to a system must also be logged in a change log that indicates the person making the change, the second individual reviewing the change, the change made, the date and time, and any approvals obtained for the change
- In addition, guidelines should define the approvals required for specific types of changes. For example, technical management approval may be required for certain changes, business approval (e.g., TAC DM) for others

2. **Recommendation:** *Audit QA and gatekeeper processes and identify gaps and improvements*

   Priority: Medium-High

   Owner: Operational Excellence

   Key Organizations and Roles: Not clear which organization could conduct an effective, objective audit.

   As noted above, there are reported gaps in QA and gatekeeper processes. Key focus for this thread would be to audit processes and identify improvements along the following dimensions:

   - Gatekeeper process and outcomes
   - Evaluation and continuous improvement of test strategy and planning activities
   - Knowledge transfer and retention
   - QA coverage, results, and gaps

3. **Recommendation:** *Develop I2R architecture, dependency, and business information flow documentation to improve change impact and risk assessment*

   Priority: High

   Owner: SIS

   Key Organizations and Roles: IT track experts, CACO, Business

   Lack of complete architectural and functional documentation has been noted as a gap by multiple groups and for multiple reasons. Lack of documentation impacts change requesters' ability to identify impacts, as well as QA's ability to help understand how to appropriately test. Steps for this recommendation include:

   - Identifying available documentation sources

- Triaging documentation gaps based on application priority and stability
- Conducting interviews and discovery sessions (assuming that technical writing resources develop the documentation, working with SIS, IT tracks, and business representatives as subject matter experts)
- Developing documentation identified as high-priority
- Identifying a long-term plan to maintain system documentation in a complete and current state.

4. **Recommendation:** *Improve IT prioritization and decision processes*
   Priority: Medium
   Owner: Operational Excellence
   Key Organizations and Roles: DLT, RMO
   Key activities along this thread include the following tasks:
   - Define mechanisms for prioritizing projects
   - Evaluate the IT funding model for delivery versus maintenance and support
   - Define the decision process for resource and budget allocations and trade-offs
   - Define relative project priorities for projects currently on the IT roadmap

5. **Recommendation:** Measure and report change management outcomes and identify ongoing improvements
   Priority: Ongoing (e.g., quarterly) activity for Operational Excellence
   Owner: Operational Excellence
   Key Organizations and Roles: RMO, DLT, CCB

11.3. Other Next Steps

This section documents other activities planned to occur after the Tiger Team transition point.

Action	Owner	Contributors	Timing
Support OnePCC implementation	May Tran	Zach May, Sherman Chiu, Danny Liu	December-March
Complete Kintana approver changes for I2R applications (linked but not dependent on OnePCC)	May Tran	Zach May, Sherman Chiu, Danny Liu	December-March
Tune risk assessment criteria and weights over time	Sherman Chiu	Iain Campbell, Trey Morris	Next two quarters
Streamline questionnaires for Risk Assessment, ARB, PCC over time to eliminate redundancies	Risk Analyst (Sherman Chiu)	ARB coordinator (Trey Morris); Gatekeeper (Shaul Johnson)	Next two quarters

11.4. Lessons Learned

Lessons learned from the conduct of this effort are listed below:

- **Consistent team membership.** The efforts of the overall program suffered repeatedly due to turnover of key resources. The Change Control team in particular became stalled at certain points of the program and needed significant re-focusing to get back on track. The eventual success of the team was helped significantly by the following factor.
- **Dedicated internal resources.** This program struggled initially due to a lack of dedicated internal resources. Certain external resources were committed 100%, but internal resources with significant participation were in extremely short supply. In some cases, internal participation amounted mostly to (in some cases infrequent) meeting attendance. Addition of a new business sponsor drove the program get the internal support it needed, and the internal participation and buy-in was subsequently much higher – and led to the team getting back off the ground and functioning extremely well.
- **Formal time commitment by all key parties.** Some critical team members were not available to the degree needed. Escalations and re-prioritizations were needed to get participation at the needed level.
- **Strong sponsorship**. This program has benefited since its inception from strong executive backing as to the importance of the program. Despite recurring resource and budget issues – including both resource limits as well as resource decision process shortcomings – the team was always able to eventually get to a solution.
- **Individual contributions**. As always, team outcome is the sum of the collective efforts of all the involved individuals. After all the resource churning was complete, the final team was a very strong team, with significant contributions across the team members both individually and as a group.
- **Streamlined decision processes**. The first three factors mentioned above began as issues that were resolved over the course of the program. Each issue was painful, bureaucratic, and time-consuming to address. For example, each resource decision needed (due to turnover or identified shortfalls) required a large number of people, and in most cases multiple discussions, to identify a resolution. A fair amount people-hours during the program was spent trying to get to resolutions for resource issues. The turnover in IT organization leadership (e.g., lack of both a director and a VP for specific periods) probably contributed in part to complexity of the discussions and decisions.

12. Appendix A. Process Specification

This section defines details for specific milestones, documents, and meetings within the revised change control process. The contents of this section are linked from an external document, which should be downloaded into the same folder as this master document for inline viewing. The source file for this section is located at: http://workspace/Livelink/livelink.exe?func=ll&objId=18601463&objAction=Open.

12.1. Milestones

This section specifies details the key PLC milestones, specifically focusing on changes. Changes are identified in **bold blue** text. The milestones described in the revised change control process are:

- Execute Commit (for projects)
- Release Commit (for tactical changes)
- Design Review
- Readiness Review (performed at release level)

Note that no change was made for the Concept Commit gate.

12.1.1. Execute Commit (projects)

Entry Criteria:	• **CCB Authorization received** • **Test Strategy document approved** • Others as documented for existing process
Required Documentation:	• **Test Strategy document** • **Risk Assessment (including ARB input if ARB review conducted)** • Others as documented for existing process
Decisions:	• No change to existing process

12.1.2. Release Commit (tactical changes)

Entry Criteria:	• **CCB Authorization received** • **Test Strategy document approved** • Others as documented for existing process
Required Documentation:	• **Test Strategy document (one per project; one per release for tactical changes)** • **Risk Assessments (one per tactical change, including ARB input if ARB review conducted)** • Others as documented for existing process
Decisions:	• No change to existing process

12.1.3. Design Review

Entry Criteria:	• **Approved Test Plan document** • Others as documented for existing process
Required Documentation:	• **Test Plan document (one per project or per track for tacticals)** • **Updated Risk Assessments (including ARB Design Review inputs, if conducted)** • Others as documented for existing process
Decisions:	• No change to existing process

12.1.4. Readiness Review

Entry Criteria:	• Testing complete and test plan criteria met • Release playbook complete • All other existing criteria as specified
Required Documentation:	• Test documentation • PCC/Gatekeeper documentation
Decisions:	• No change to current process • **Note: Production migration cannot occur without CCB approval subsequent to the Readiness Review** o In cases, CCB may attend Readiness Review and make the CCB production migration decision in the meeting

12.2. Meetings

This section specifies details for decision and review meetings within the revised process. Decisions related to passage or not through key PLC milestones are reflected in the Milestones section above.

12.2.1. CCB Authorization

CCB authorization is a required step in the Analysis phase. **Execute Commit (EC) is not valid for TS/I2R IT projects without CCB authorization.** For minor (tactical) releases, Release Commit (RC) is not valid without CCB authorization.

Prerequisites:	• Change Request created for the requested change (Empower, CR, I2R) • BRD, Project Agreement, **Risk Assessment**, ARB review, **Test Strategy** complete

Inputs:	• **Email for each Change Request containing the change reference (Empower ID, CR #, I2R #)** • **Risk Assessment** • **ARB review input (incorporated into revised Risk Assessment)**
Decisions:	• **Identify whether change has been sufficiently described to merit scheduling and identification of governance path** • **Authorize (or do not Authorize) reviewed change (prerequisite for Execute Commit for projects, or for Release Commit for tactical releases)**
Outputs:	• **Change calendar (deployment time for the change)** • **Governance path** • Decisions communicated to stakeholders via alias i2r-ccb-comms

12.2.2. CCB and RMO Stage Approval

For planned releases, RMO now owns the responsibility for approving stage migration. The RMO lead, in concert with the release manager and track leads, has sole discretion for managing and approving the release stage deployments. This authority extends to both C3 and non-C3 releases, as well as to both major and tactical releases.

CCB will retain authority for managing approval to stage environments for release exceptions. Those migrations will be reviewed and dispositioned in CCB meetings, as they are today.

Non-EBF changes shall not be deployed to stage environments without either CCB or RMO approval, per the above responsibilities.

Details for the CCB release exception stage migration are provided in the table below:

Prerequisites:	• **Design-phase Risk Assessment complete** • **Test Plan complete** • Development of code to be migrated complete
Inputs:	• **Change Request information for the change to be reviewed (Empower, CR, I2R)** • **Design-phase Risk Assessment**
Decisions:	• Proceed with stage migration or not
Outputs:	• Decisions communicated to stakeholders via alias i2r-ccb-comms

12.2.3. CCB Recommendation for Production

Non-EBF changes shall not be deployed to production environments without CCB approval.

Prerequisites:	• Testing complete • **Gatekeeper review complete and passed** • Release playbook complete and ready • Readiness Review complete • **EMAN CR for the change or set of changes**
Inputs:	• **Change Request information for the changes to be reviewed (Empower, CR, I2R, release)**
Decisions:	• Proceed with production migration or not
Outputs:	• CR approval • Decisions communicated to stakeholders via alias i2r-ccb-comms

12.2.4. Test Strategy Review

Prerequisites:	• **Test Strategy complete in draft form** • Initial ARB engagement complete • **Initial Risk Assessment performed and inclusive of ARB results**
Inputs:	• Functional specifications • **ARB review output** • **Risk Assessment** • Business Requirements Documents
Meeting Attendees:	• **QA, business, RMO, architecture, IT, risk analyst**
Decisions:	• **Identify key gaps in the Test Strategy and plan for resolution** • **If ready, approve document**
Outputs:	• **Approved Test Strategy document**

12.2.5. Test Plan Review

Prerequisites:	• Test Plan complete in draft form • Technical documentation complete and available • Design Review with ARB participation complete (if required for identified Risk Rating) • **Risk assessment updated based on Design phase input from IT (and ARB, if applicable)**
Inputs:	• **Test Strategy** • **Risk Assessment** • Technical documentation

Meeting Attendees:	• QA, business, RMO, architecture, IT, risk analyst
Decisions:	• Identify key gaps and plan for resolution • If ready, approve document
Outputs:	• **Approved Test Plan document**

12.3. Documents

This section specifies details for new and revised documents, focusing primarily on areas of change for existing documents.

12.3.1. Risk Questionnaire (Analysis Phase)

Author:	• Change Requester (IT)
Inputs:	• Business requirements documentation • Functional specification documentation
Required Content:	• Description of system changes to be made, per the questionnaire – Section 1 only
Template:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18313646&objAction=Open
Approvers:	• Risk Analyst
Archived at:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18324496&objAction=browse&sort=name

12.3.2. Risk Assessment (Analysis Phase)

Author:	• Risk Analyst
Inputs:	• **Risk Questionnaire** • **ARB review content, if applicable** • Requirements documentation, functional specification documentation, project agreement as needed for reference
Required Content:	• Identification of the change's Risk Rating, based on degree/type of change, system priority, stability, etc. • Analysis of change risk versus benefit • Identification of key areas of risk • Identification of needed mitigations and implications
Template:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18565108&objAction=Open
Approvers:	• N/A
Archived at:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18558059&objAction=browse&sort=name

12.3.3. Test Strategy

Author:	• QA
Inputs:	• **Risk Assessment** • **ARB review content, if applicable** • Functional specifications • Business requirements documentation
Required Content:	• Key areas of risk and implications • Summary of test strategy / approach by key business or functional area
Template:	• http://workspace/Livelink/livelink.exe?func=ll&objId=18608498&objAction=Open
Approvers:	• Business, QA, IT, RMO, Architecture, Risk Analyst
Archived at:	• Varies per release

12.3.4. Risk Questionnaire (end of Design Phase)

Author:	• Change Requester (IT)
Inputs:	• **Initial Risk Questionnaire** • Technical documentation

Required Content:	• Description of system changes to be made, per the questionnaire:
	  o Review and revise Section 1
	  o Complete Section 2

Template:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18313646&objAction=Open
Approvers:	• Risk Analyst
Archived at:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18324496&objAction=browse&sort=name

12.3.5. Risk Assessment (end of Design Phase)

Author:	• Risk Analyst
Inputs:	• **Revised Risk Questionnaire** • **For projects: ARB Design Review input, if ARB participation in Design Review**
Required Content:	• Identification/revision of the change's Risk Rating, based on degree/type of change, system priority, stability, etc. • Analysis of change risk versus benefit • Identification of key areas of risk • Identification of needed mitigations and implications
Template:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18565108&objAction=Open

Approvers:	• N/A
Archived at:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=18558059&objAction=browse&sort=name

12.3.6. Test Plan

Author:	• QA
Inputs:	• **Risk Assessment** • **Test Strategy** • Technical documentation
Required Content:	• Unchanged from current process – one test plan per project or per track for tacticals
Template:	• http://workspace/Livelink/livelink.exe?func=ll&objId=18618143&objAction=Open
Approvers:	• Business, QA, IT, RMO, Architecture, Risk Analyst
Archived at:	• Varies per release

12.3.7. PCC Document

Author:	• Change Requester (IT)
Inputs:	• Test documentation
Required Content:	• Same as in current process
Template:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=17336495&objAction=Open
Approvers:	• Gatekeeper
Archived at:	• https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=9871746&objAction=browse&sort=name

13. Appendix A. Supplementary Process Information

13.1. Standard Production Approval Lead Times

The preferred deployment window is on Friday night / Saturday morning. Lead times for a Friday night deployment are shown in the table below.

Activity	Responsible Party	Cutoff Time
Complete PCC template and testing for STAGE/TEST environment	Project Manager	Wednesday, 11AM PST
Complete PCC audit, inform Change Requestor of audit results	Gatekeeper	Wednesday, 5PM PST
Obtain CCB approval for deployment to production	Project Manager	Thursday, 2PM PST
Add approved change request number and associated Kintana package(s) to production deployment scope document- send document to SCM Build Team, SCM Operations, Gatekeeper, C3-Support alias	CCB Coordinator	Thursday, 3PM PST
Have C3 downtime packages ready in Kintana for Gatekeeper approval	Developer	Friday, 10AM PST
Provide Kintana migration approvals for C3 downtime packages	Gatekeeper	Friday, 11:30AM PST
Have C3 non-downtime or non-C3 packages ready in Kintana for Gatekeeper approval	Developer	Friday, 3PM PST
Provide Kintana migration approvals for C3 non-downtime and non-C3 packages	Gatekeeper	Friday, 4:30PM PST
Record Gatekeeper comments and decisions into production deployment scope document- archive document	Gatekeeper	Friday, 5:00PM PST

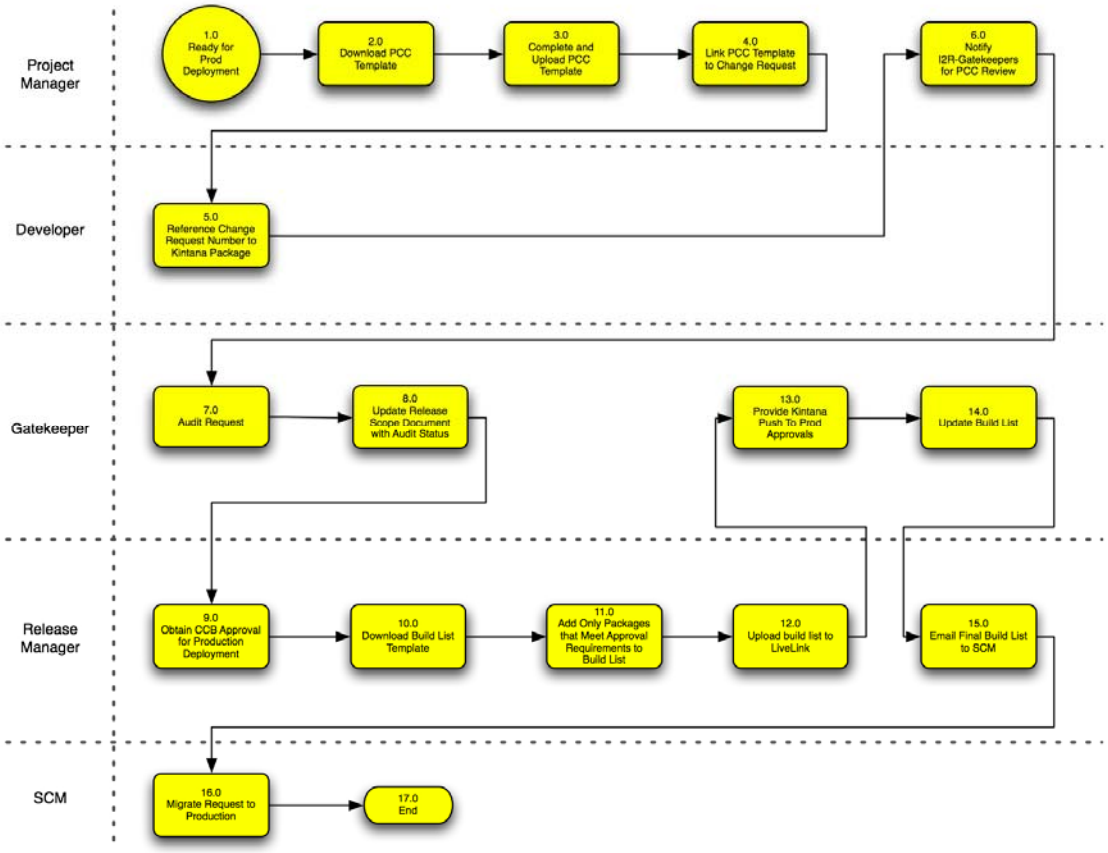
13.2. Non-Standard Production Approval Lead Times

CCB may approve production deployment during a non-standard deployment window. Lead times for non-standard production deployment are shown below.

Activity	Responsible Party	Cutoff Time
Complete PCC template and testing for STAGE/TEST environment	Project Manager	11 AM PST, 2 days prior to intended deployment window
Complete PCC audit, inform Change Requestor of audit results	Gatekeeper	5PM PST, same day review request received
Obtain CCB approval for deployment to production	Project Manager	2PM PST, 1 day prior to intended deployment window
Add approved change request number and associated Kintana package(s) to production deployment scope document- send document to SCM Operations, Gatekeeper, C3-Support alias	CCB Coordinator	3PM PST, 1 day prior to intended deployment window
Have evening packages ready in Kintana for Gatekeeper approval	Developer	2PM PST, on intended deployment day
Provide Kintana migration approvals for evening window packages	Gatekeeper	4:30PM PST, on intended deployment day
Record Gatekeeper comments and decisions into production deployment scope document- archive document	Gatekeeper	5:00PM PST, on intended deployment day

13.3. Gatekeeper Review Process

The Gatekeeper review process has not changed in the 1.0 Change Control process. The process flow is shown below.[17]



[17] Source file: Planned Release Prod Deployment 120606. See the references section (Section 15) for links to additional information regarding the Gatekeeper process

14. Appendix B. Glossary

Term	Definition
Boundary Application	Any application, either downstream or upstream to the project scope, that has direct or indirect impact to code change, data structure change, data change, configuration change or any other change which has impact to it is termed as Boundary application and needs to be dealt as part of project scope. The Test Strategy document shall define in detail the boundary application and the testing model for each.
Change Control Process Team	Key constituents executing and managing the change control process post-go-live. Includes at a minimum QA (Moe Jabri), CCB (Iain Campbell), Risk Analyst (Sherman Chiu), ARB (Trey Morris), CACO (Chris Thomas or designee)
Emergency Bug Fix (EBF)	Emergency Bug Fixes (EBFs) are immediate changes to address outstanding P1 or P2 Alliance cases (i.e., system stability issues) that are interfering with the operational status of a system.
Project	Projects generally refer to larger system changes that appear on the IT roadmap. Sometimes these changes are called “CFPs” (for “Client Funded Projects”). Projects are generally captured in the EmPower software tool. A project consists of planned system changes that are expected require more than $50K to complete, including development work, QA, and any project management required.
Release Exception	Release exceptions refer to system changes that are deployed in between planned releases.
Tactical	Tactical changes refer to smaller, short-lead changes that are included in planned releases. C3 minor releases usually (but not always) consist only of tacticals. C3 major releases include projects as well as tacticals. Tactical changes are frequently captured in the I2R request tool. Specifically, tactical changes are planned system changes that are expected require less than $50K to complete, including development work, QA, and any project management required.
Test Case	A test case defines a series of steps to test a particular requirement. It usually takes many test cases to test a single requirement. Test case consists of the following - Description (test objective, prerequisites, reference to corresponding requirements or use cases), Test steps and expected results. It may also has attachments (e.g. SQL query, screen shots etc) to aid the tester during execution.
Test Plan	Document describing the project overview, testing scope (in scope and out of scope items), dependencies, issues, risks, testing timeline and high level test scenarios. This document is prepared by the QA coordinator for the project and is reviewed by the IT PM, SME, Business PM, Risk Analyst, RMO, and Architecture. A formal review meeting with and sign-off from those individuals is required.

Term	Definition
Test Scenario	Test scenario is the definition of a set of test cases designed to validate a particular business requirement. There can be many test scenarios to test one single requirement. Test scenarios are used by CA QA as a high level summarization of all the test cases that will be developed as part of any project. It helps to articulate the scope of testing as perceived by the QA team. It also makes it easier for the Business and IT teams to review and confirm that the scope identified by QA team covers all the necessary scenarios.
Test Strategy	Document describing the overall approach to the end-to-end testing process and containing the following: • Scope of the change, summary of implications as to risks and impacts, and mitigations • Scope and objective of testing including Boundary applications • Summary of components to be tested and test approach for each • Typical model that will be followed for the project • Entry and Exit criteria for each phase of the testing • Requirements trace matrix • Defect severity and priority definition • Types of testing (e.g. Unit, String, Smoke, System, Performance, Regression etc.) • Test execution and code freeze schedule • High level testing environment
Risk Assessment	The process framework by which changes are assessed as to risk and impact and both governed and tested accordingly
Risk Questionnaire	An MS-Excel based questionnaire completed by IT change requesters to provide information about the change to the Risk Analyst, and to support assessment of the risk and impact of the change to CCB for Authorization
CCB Authorization	Change control process step where the governance path for the change and the change window are determined
CCB Stage Approval	Change control process step where the CCB approves (or does not approve) migration of code into a Stage environment. CCB performs stage approval only for release exceptions; RMO approves otherwise
CCB Production Approval	Change control process step where the CCB approves (or does not approve) migration of code into a Production environment. Changes of the lowest Risk Rating level do not require CCB Production Approval

15. Appendix C. References

Reference	Link
MS Visio Process Flows	http://workspace/Livelink/livelink.exe?func=ll&objId=18207159&objAction=Open
Application Repository	http://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=10726066&objAction=browse&sort=name
OnePCC overview and process flows	http://workspace/Livelink/livelink.exe?func=ll&objId=18399094&objAction=browse&sort=name
QA process documentation	http://workspace/Livelink/livelink.exe?func=ll&objId=18390885&objAction=Open
I2R Health Reports (excludes TACSUNS until Nov06)	http://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=10398197&objAction=browse&sort=name
I2R P1/P2 case tracking files (managed by CACO) – excludes TACSUNS and TopX tools	http://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=12957834&objAction=browse&sort=name
Change-related P1/P2 cases in Q107	http://workspace/Livelink/livelink.exe?func=ll&objId=18639273&objAction=Open
I2R Stabilization Main Folder	http://workspace/Livelink/livelink.exe?func=ll&objId=15495103&objAction=browse&sort=name
Gatekeeper Toolkit	https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=12858744&objAction=browse&sort=name
Gatekeeper/PCC Specifics	https://ework.<company>.com/Livelink/livelink.exe?func=ll&objId=12501140&objAction=Open
Electronic version of this file	http://workspace/Livelink/livelink.exe?func=ll&objId=18608482&objAction=Open

16. Revision History

Date	Author	Version	Change Description
21Dec06	Melissa Liu	1.0	Initial Version