

NASA

**IT Change Management Process Document
Version 1.0**

April 16, 2009

Table of Contents:

Document Abstract	3
Document Owner	3
Revision History.....	3
IT Change Management Purpose	4
IT Change Management Scope.....	4
IT Change Management Process Description.....	4
Emergency IT Change Management Process Description	16
IT Change Management Process Exemptions.....	16
IT Change Management Roles and Responsibilities	17
IT Change Requests.....	18
Sample IT Change Request Form.....	18
Authorization of IT Changes.....	19
IT Change Categorization Table.....	19
Building of IT Changes	19
Release of IT Changes.....	20
IT Change Management Performance Measures.....	20
IT Change Management Key Integration Points	21
Document Maintenance	21

Document Abstract

This document provides all involved parties (including staff, management, partners, providers, and contractors), regardless of physical location with a guide and reference to **NASA's** IT change management processes, procedures, and standards.

Document Owner

The IT change management process document is owned by the Architecture and Infrastructure Division within the NASA Office of the Chief Information Officer.

Revision History

Version	1.0
Revision Date	4/16/2009
Authors	
Changes	
Approval:	
Next Revision:	

IT Change Management Purpose

NASA recognizes the need to establish reasonable guidelines for the effective use, management, and maintenance of underlying IT change management. In doing so, **NASA** seeks to protect the integrity of its production environment and ensure adherence to NASA standard IT service management practices.

The purpose of this document is to provide all involved parties (including staff, management, partners, providers, and contractors), regardless of physical location with a guide and reference to **NASA's** IT change management processes, procedures, and standards.

This document also serves to ensure that all parties involved in **NASA's** IT change management processes, procedures, and standards, understand the requirements associated with NASA's IT change management processes, procedures, and standards.

IT Change Management Scope

This document is intended to cover all IT changes associated with **NASA's** IT environment including, but not limited to:

- HW
- SW
- Operating Systems
- Applications
- Telecommunications
- Networks
- Systems
- Patches, Upgrades, Modifications
- People/Organizational Structure
- Process
- Service Levels

IT Change Management Process Description

The IT change management process at **NASA** is a complex set of tasks, activities, functions that manage any/all HW/SW alterations made to the IT environment. The IT change management process is responsible for the management of IT change requests, development of the IT alterations, as well as the testing and distribution of those IT changes.

The IT change management process at **NASA** is comprised of the following tasks:

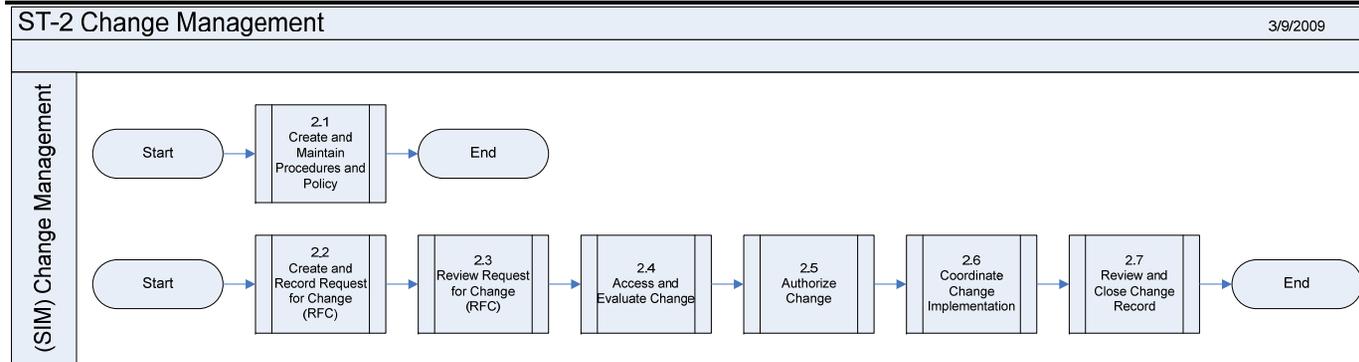
- Requests for change

- Change requests are the ‘notice’ to others within IT that an alteration to the IT environment. Change requests may come from a variety of individuals within the IT community, and are necessary for effective tracking and information management. Making a change request often occurs in a ticket and workflow management tool (e.g., Remedy/BMC, Peregrine/HP).
- Categorization of changes
 - Categorization of changes is essential to ensure that changes are properly prioritized and that resources are most effectively allocated. Changes are often categorized based on impact to the business, cost of change, potential risks to service performance resulting from the change.
- Change risk assessment
 - Change risk assessments are done to assess potential risks to service/the IT environment resulting from proposed changes. Change risk assessments are used to minimize the impact of problems/incidents resulting from changes. Risk assessments facilitate change authorization and scheduling and may be used as well in the development of a change categorization schedule.
- Authorization of changes
 - Authorization of changes is often done as part of the Change Advisory Board (CAB) meeting, however, in emergency situations, changes may be authorized by parties that have been identified as appropriate representatives. Changes that have proven not to impact the IT environment negatively (e.g., service impact, change cost) may be pre-authorized by the CAB.
- Scheduling of change builds
 - Scheduling of change builds helps to prioritize change and associated resources. Higher impact changes may be authorized by the CAB, while lower impact changes may be scheduled by those performing the change itself (note: self-scheduling is to be performed only on ‘pre-authorized’ changes identified by **NASA**.)
- Planning of change builds
 - Once the change is authorized and scheduled, those responsible for building and executing the change are required to put a change plan together. The change plan articulates: what the change encompasses, resources, official timing, back-out procedures, etc.
- Change builds/development
 - The change build is the actual construction of the change components. This function may be performed by application development, various operations personnel, etc. The change build does not include the release/implementation of the change.
- Testing of change builds (e.g., unit testing)
 - This is the test of the items that have just been built. Often referred to as unit testing.
- Packaging of changes for release to operations

- Packaging of changes for release to operations is performed by those responsible for the change build. This function is often the application development interpretation of release management, but may be performed by operations personnel as well.
- Requests for operational release
 - By formalizing the request for a release of a newly built item into operations, the organization ensures a more formal hand-off between applications development and operations.
- Validation of operational release requests
 - Validation of operational release requests is performed by operations to ensure all appropriate information (e.g., timing requirements, performance expectations, risk assessments) are included and appropriate.
- Review of operational support requirements
 - Operational support requirements are reviewed for each new release to ensure that operations can handle and appropriately support the new release. Support requirements may include key support personnel, platform information, etc.
- Comparison against operational histories
 - Comparison of operational histories seeks to compare the new release with previous “similar” releases, identifying any problem/interruption/resolution knowledge/experience for previous releases that may be leveraged for the new release.
- Assessment of operational support capabilities
 - Assessment of operational support capabilities is the final step to ensure that operations is appropriately staffed to stage, implement, and support the release.
- Risk mitigation planning
 - Risk mitigation planning is required to plan for potential disruptions in service due to changes being released into the existing environment, and to design actions necessary for the resumption of service. This planning will be handed to those responsible for distribution into the environment.
- Communication of release information to associated parties
 - Once a change release has been requested of operations, and initial histories/requirements have been examined, those responsible for distributing the release into the environment must be notified.
- Documentation of release plan
 - Documentation of the release plan incorporates all necessary requirements and resources for the distribution itself.
- Scheduling of releases to production
 - Scheduling of releases to production is the final schedule for when the change/release gets pushed into production.
- Assignment of release activities
 - Release activities are assigned for distribution.

- Configuration/packaging of release
 - Configuration/packaging of releases is the final packaging of the release. Whereas application development's interpretation of release occurs earlier in this lifecycle (see Packaging of changes for release to operations), this packaging includes all release components necessary for distribution into the environment.
- Testing of change releases to production (e.g., load testing)
 - Testing of change releases to production takes the change/release and tests it against the production environment.
- Distribution of the change (electronic and/or physical)
 - Distribution of the change is the actual drop/release of the change into the production environment.
- Change quality assurance
 - Quality assurance occurs following the drop of the change into the production environment. This function may be performed by a variety of IT personnel, but traditionally the function is best performed by those performing the actual distribution functions, or others in the operations environment who may be most familiar with the performance of the production environment.
- Closure of change tickets
 - Once changes have been executed, distributed, and checked for quality, the change ticket should be returned to the ESD for customer surveys and subsequently closed.

IT Change Management Flow



Purpose, Goals and Objectives:

The **purpose** of Change Management process is to ensure that:

- (1) Standardized methods and procedures are used for efficient and prompt handling of all changes
- (2) All changes to service assets and configuration items are recorded in the Configuration Management System
- (3) Overall business risk is optimized.

The **objective** of the Change Management process is to ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

The **goals** of Change Management are too:

- (1) Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work
- (2) Respond to the business and IT requests for change that will align the services with the business needs.

Triggers:

Key trigger categories:

- (1) Strategic changes
- (2) Changes to one or more services
- (3) Operational change
- (4) Changes to deliver continual improvement

Inputs:

Changes may be submitted as a Request for Change (RFC), often with an associated change proposal that provides the detail of how the change will happen.

- (1) Policy and strategies for change and release
- (2) Request for Change
- (3) Plan (change, transition, release, deployment)
- (4) Current change schedule and Projected Service Outage (PSO)
- (5) Current asset or configuration item
- (6) As-planned configuration baseline
- (7) Test results, test report and evaluation report

Primary Interfaces:

Service Management processes may require change and improvements.

Many will also be involved in the impact assessment and implementation of service changes, as listed below:

- Asset and Configuration Management
- Problem Management
- IT Service Continuity
- Security Management
- Capacity and Demand Management
- Release and Deployment Management

Outputs:

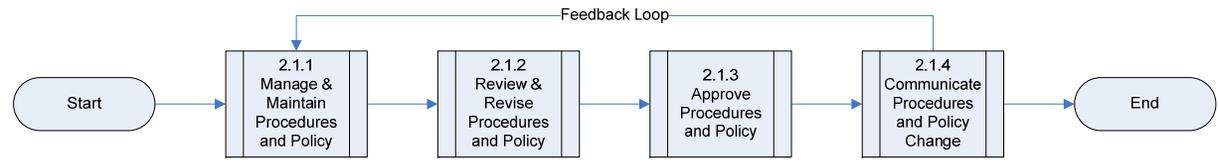
- (1) Rejected (Request for Change) RFCs
- (2) Approved RFCs
- (3) Change to the Services
- (4) Change Schedule
- (5) Revised Projected Service Outage (PSO)
- (6) Authorized Change Plans
- (7) Change Decisions and Actions
- (8) Change Documents and Records
- (9) Change Management Reports

ST-2.1 Design and Maintain Change Management Procedures and Policy

3/9/2009

NASA Business
User Community

(SIM) Change
Management



Other NASA
Retained Authority

Provider – Primary
Services

Provider – Support
Services

ST-2.2 Create and Record Request for Change (RFC)

3/9/2009

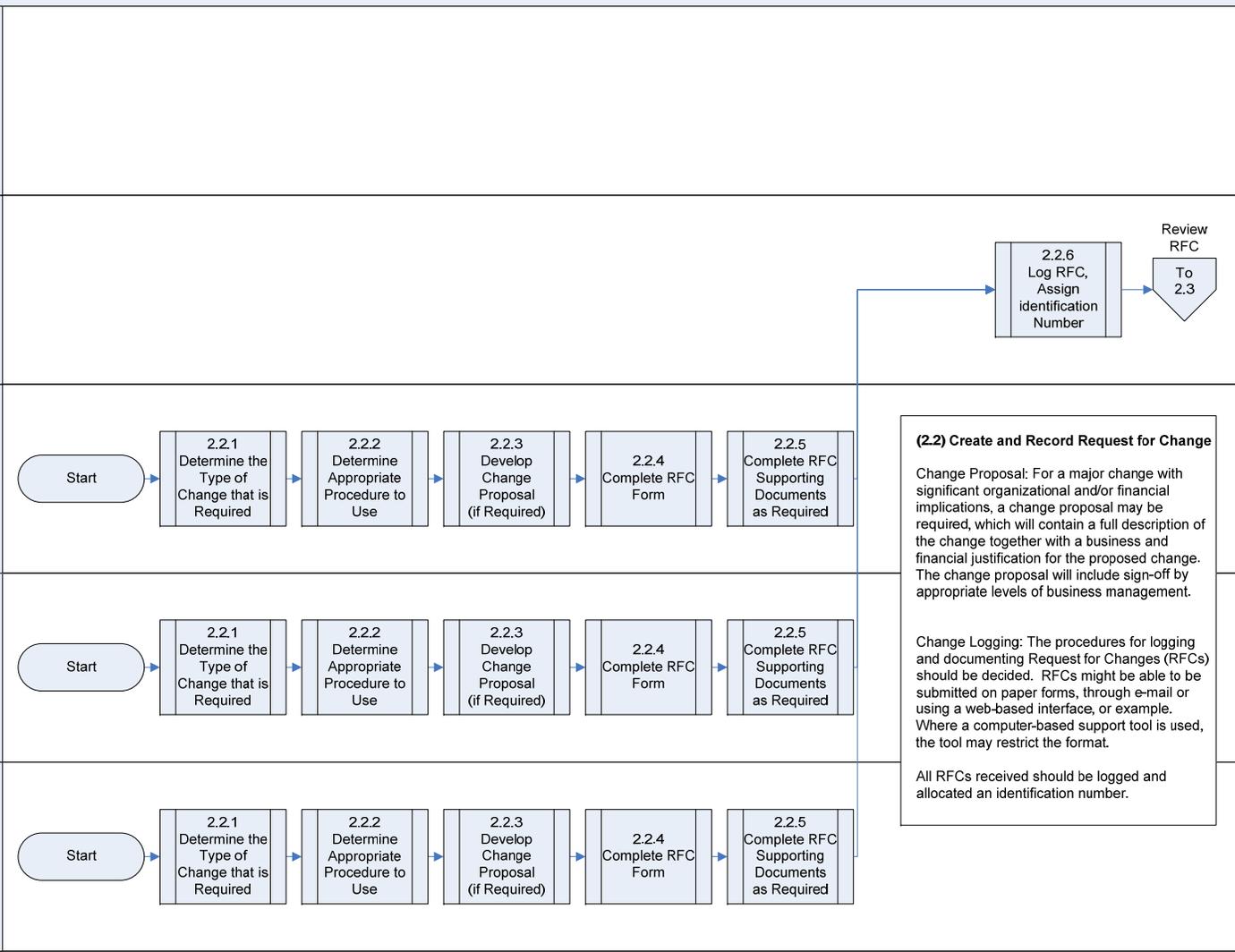
NASA Business
User Community

NASA ESD TTS

Other NASA
Retained Authority

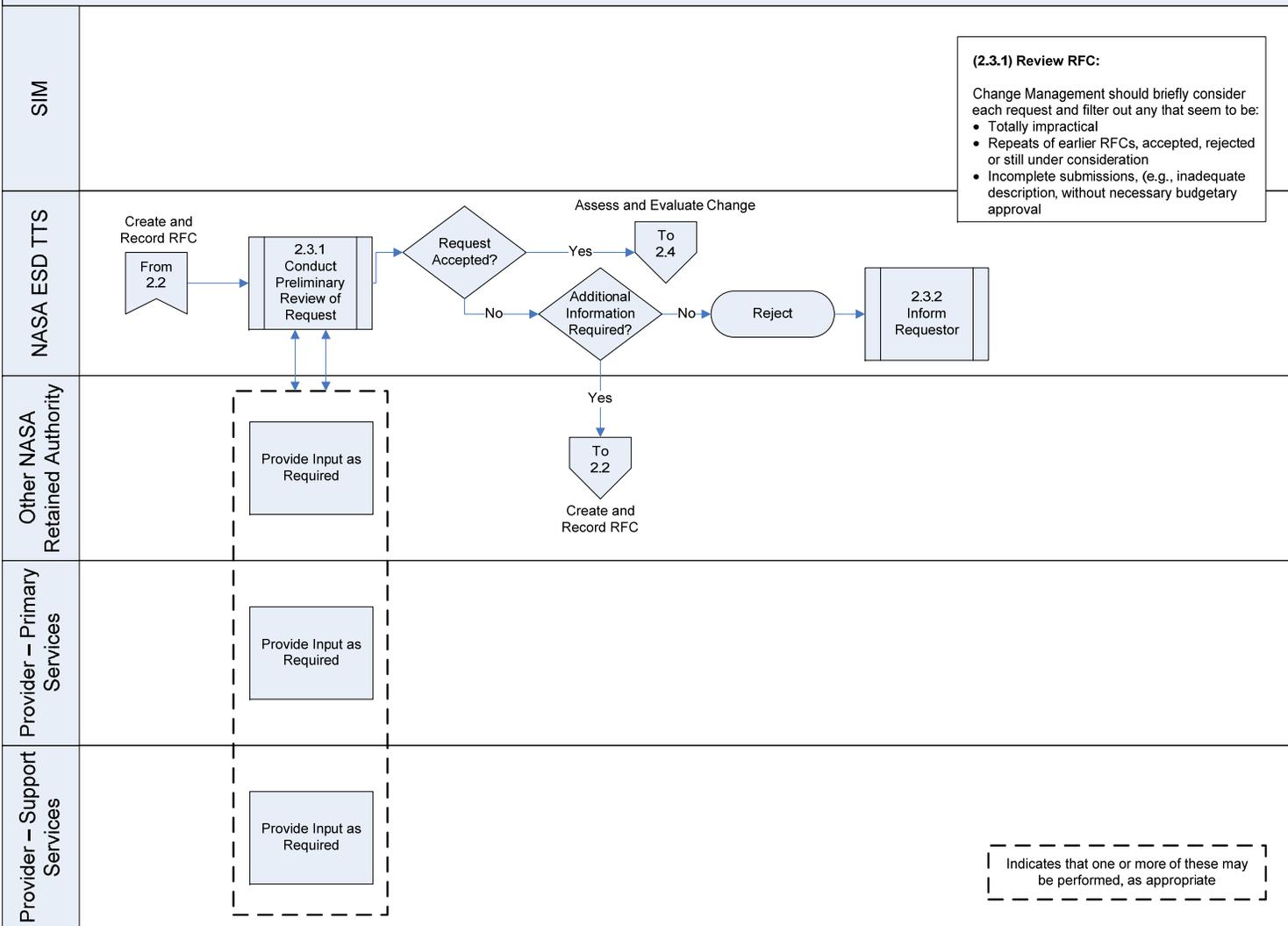
Provider – Primary
Services

Provider – Support
Services



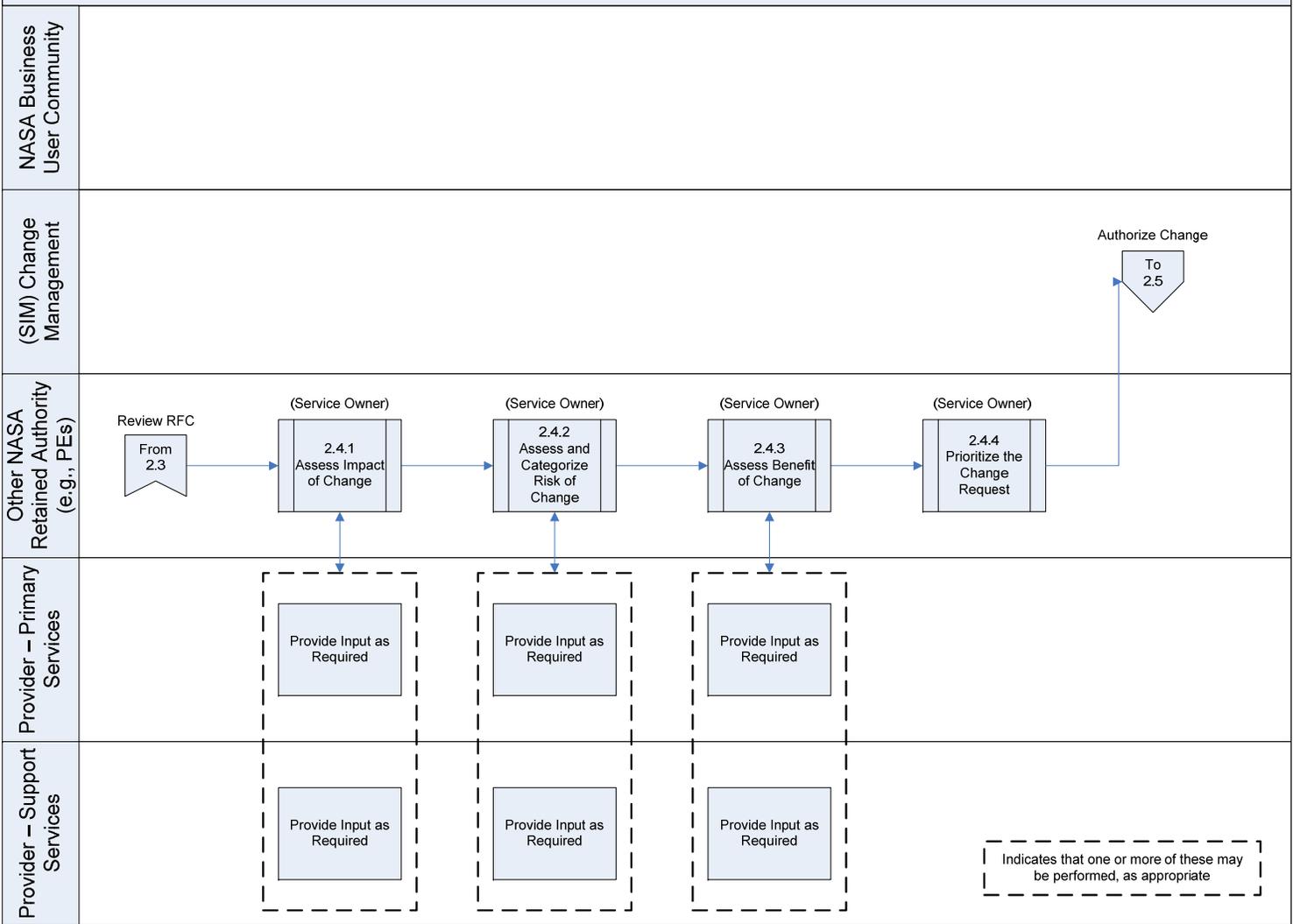
ST-2.3 Review Request for Change (RFC)

3/9/2009



ST-2.4 Assess and Evaluate Change

3/9/2009



ST-2.5 Authorize Change

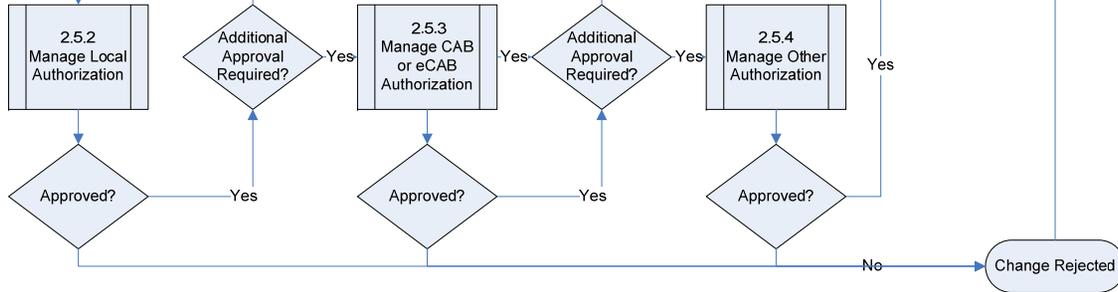
3/9/2009

NASA
Business
Customers

(SIM) Change
Management



Other NASA Retained Authority
{e.g., PEs, EA, SMEs}

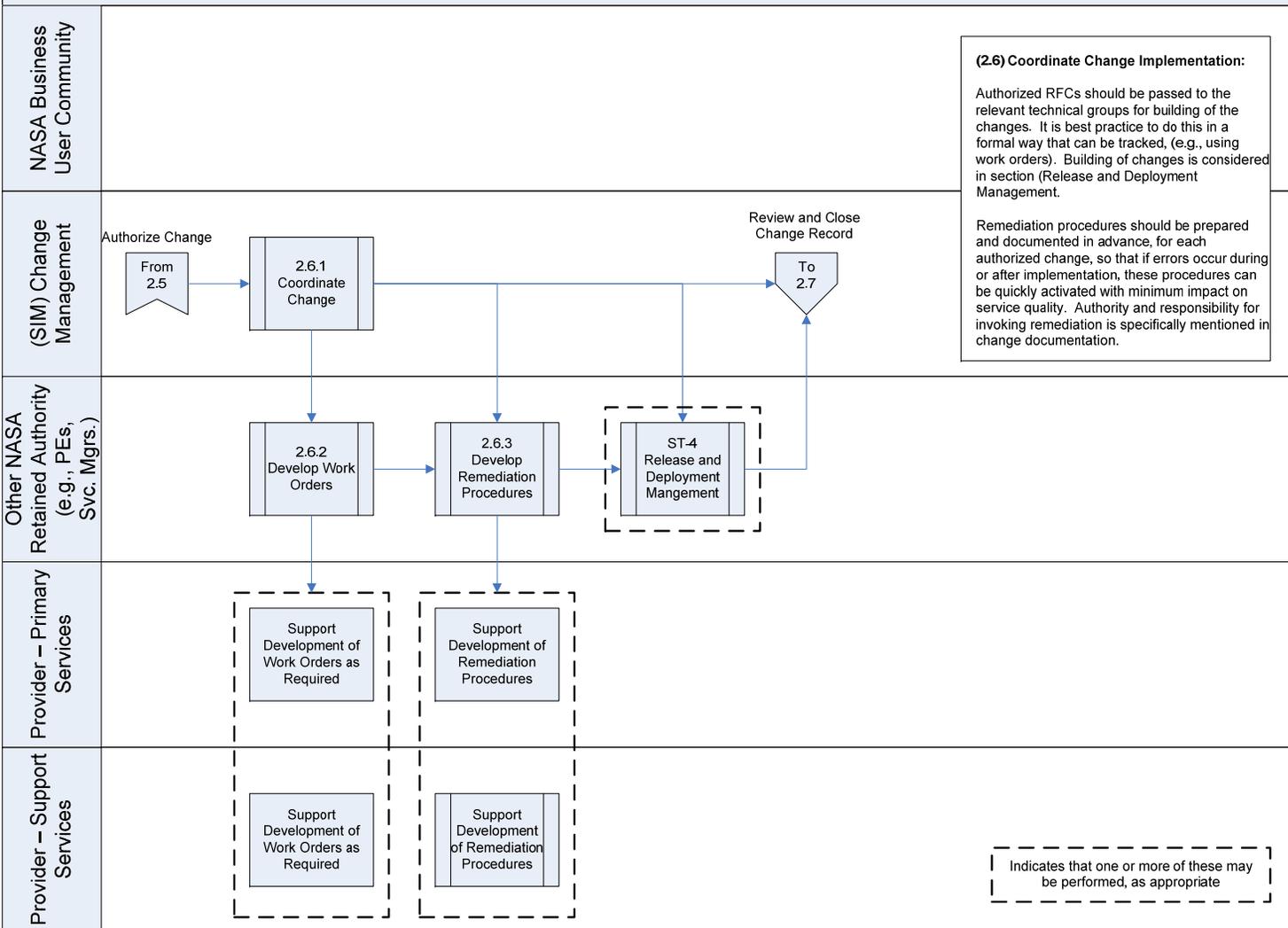


Provider –
Support
Services

Provider –
Primary
Services

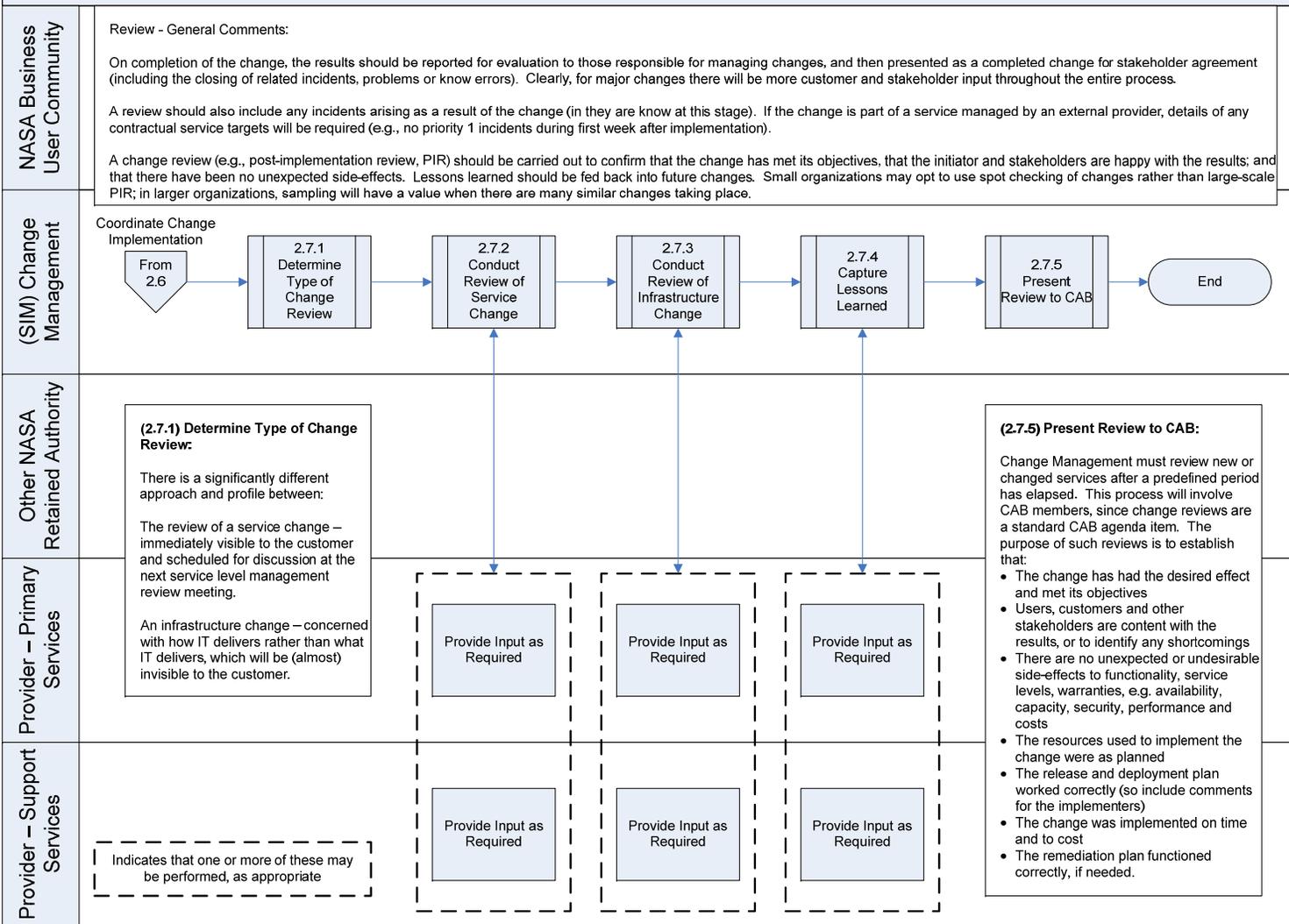
ST-2.6 Coordinate Change Implementation

3/9/2009



ST-2.7 Review and Close Change Record

3/9/2009



Emergency IT Change Management Process Description

The acceptance of “emergency” IT changes tends to result in a minimization of appropriate authorization, scheduling, testing, etc., and often results in the emergency change process becoming the standard rather than the exception. **NASA** recognizes that emergency IT changes will occur and must be accounted for in its IT change management process structure. To manage emergency IT changes as effectively as possible, **NASA** will require emergency IT changes to follow the “normal” IT change process described earlier, with the allowances described in the following table:

Emergency Change Type	Authorization/Timing/Review
Emergency Change Description	<ul style="list-style-type: none"> • Authorizations required • Timing expectations • Quality review
Emergency Change Description	<ul style="list-style-type: none"> • Authorizations required • Timing expectations • Quality review
Emergency Change Description	<ul style="list-style-type: none"> • Authorizations required • Timing expectations • Quality review
Emergency Change Description	<ul style="list-style-type: none"> • Authorizations required • Timing expectations • Quality review
Emergency Change Description	<ul style="list-style-type: none"> • Authorizations required • Timing expectations • Quality review

IT Change Management Process Exemptions

This process document does not apply to:

- IT changes made by, or on behalf of, the business for which **NASA**'s IT department does not have knowledge of/involvement with.

IT Change Management Roles and Responsibilities

A number of roles and responsibilities have been identified as essential to the IT change management process. The purpose of this section is to define those functional roles and responsibilities necessary for effective IT change management, including but not limited to, **NASA's** staff, management, partners, providers, and contractors, regardless of physical location, involved in making IT changes to **NASA's** IT environment.

Roles	Responsibilities
(SIM) Change Management Process Owner	<ul style="list-style-type: none"> • Responsible for the documentation, modification, and update of all IT change management process documentation • Responsible for assuring that the change process meets organizational performance expectations • Ensures that individuals/groups adhere to the change process • Accountable for the efficiency, effectiveness, and accountability of the process • Responsible for change management performance reporting
Change Coordinator	<ul style="list-style-type: none"> • Leads weekly Change Advisory Board (CAB) meetings • Accountable for change schedule in concert with CAB • Identifies when to update the change process • Reviews change requests for accuracy/completeness • Assists with change management reporting and documentation • Assists with change management scheduling and communication
Change Requester	<ul style="list-style-type: none"> • Submits change requests • Responsible for communicating all requirements, risks, and timing issues associated with the change
Change Developer	<ul style="list-style-type: none"> • Designs change • Provides test component information • Responsible for back-out plan • Provides implementation instructions
Change Implementer	<ul style="list-style-type: none"> • Puts the change into production • Assures change success
Change Advisory Board	<ul style="list-style-type: none"> • Approves all high risk change requests • Reviews all change requests in relation to risks • Responsible for change scheduling • Resolves all change scheduling conflicts • Identifies appropriate changes for "pre-approval"

IT Change Requests

IT change request forms (see sample IT change request form) are to be filed for any HW/SW development initiative and/or any alteration to be made to the production environment.

- IT change requests that have not been “pre-authorized” by the change advisory board must be reviewed by the appropriate authorizing body (see change categorization table) in addition to entry of a formal IT change request.
- Low risk IT changes which have been “pre-authorized” by the change advisory board are required to have a change request entered, but do not require review by the change advisory board.

IT change tickets are expected to be filed prior to the development and implementation of the change itself.

Sample IT Change Request Form

Submission #	
Submission Date	
Requestor's information (name, phone, dept.)	
Change type	
Description and identity of item(s) to be changed	
Reason for change	
Change priority	
Risk/impact and resource assessment	
Business applications/services affected	
Customers affected	
Systems affected	
Estimated downtime	
CAB recommendations	
Notification list	
Authorization signature	
Authorization date and time	
Scheduled implementation date	
Details of change	
Back-out plan	
Actual implementation date and time	
Review date	
Review results	
Change status – logged, assessed, rejected, accepted, on hold	
Notes	

Authorization of IT Changes

IT change requests must be authorized by the appropriate authorizing body. IT change authorization should use the change categorization table as a guide. The following summarizes the change categorization table:

IT changes may be rejected for any of the following reasons:

- if the IT change request is submitted without the required information (e.g., risk assessment, timing estimates)
- if the IT change request is submitted outside of the authorized change windows
- if the IT change request conflicts with other changes currently in progress
- if the IT change is likely to negatively impact the production environment
- if the IT change requires an undue amount of resource (e.g., time, person-hours)

IT Change Categorization Table

Level	Change Characteristics:	Level of Authorization:
1	<ul style="list-style-type: none"> • High risk • High possibility of major business impact • No potential for back-out • Lengthy change 	CAB and Business
2	<ul style="list-style-type: none"> • High risk • Moderate possibility of major business impact • Complex back-out • Lengthy change 	CAB
3	<ul style="list-style-type: none"> • Moderate risk • Moderate back-out • Moderate length change 	CAB or Manager
4	<ul style="list-style-type: none"> • Low risk • Moderate back-out • Moderate length change 	Manager
5	<ul style="list-style-type: none"> • Low risk • Known requirements • Easy back-out 	"Pre-Authorized"

Building of IT Changes

IT change builds are expected to follow all reasonable and customary planning, scheduling, build/development, and documentation to ensure changes are: built

to specification; cause minimal impact to the IT production environment; and meet regulatory requirements/expectations.

Documentation of IT change builds will be stored in [Configuration Management System].

Release of IT Changes

A system of checks and balances must be in place regarding the release of IT changes into the production environment. As such, personnel responsible for the development of any level 1-3 changes may not release those changes into the production environment themselves unless authorized in an emergency scenario.

Release requests are expected to be presented to the “operational release” team, and must be accompanied by the appropriate tested release component, and risk analysis, documentation.

Requests for the release of level 1-3 IT change releases should be given a minimum of 3 business days.

IT Change Management Performance Measures

NASA will measure and maintain the performance of its IT change management process through the NASA Enterprise Service Desk with the following performance measures:

- # of changes implemented per period (i.e., Week)
 - By item
 - By type/service
- # /% of successful/unsuccessful changes
- Reasons for change
 - User requests (%)
 - Enhancements (%)
 - Service call/incident/problem fixes (%)
- # of changes backed-out by reason
- # / % of incidents with change as the root cause
 - Broken down into problem/severity levels
- # of requests for change
- # / % of requests for change rejected
- #/% of emergency changes
- # / % of changes scheduled and executed on time
- # of changes resulting in a call to the service desk
- # of change/problem requests relating to one config item
- Gross number of changes and trends

- # / % of changes executed outside normal change process
- Change backlogs, broken down by configuration items
- Cost per change
- #/% of change requests generated by the business
- Ratio of accepted to rejected change requests
- % of emergency fixes for which the change process was not applied retroactively

IT Change Management Key Integration Points

Effective IT change management requires significant integration between those technology and business communities that request, build, test, implement, and monitor IT changes. As such, the IT change management process should include, but not be limited to, the following process integration points:

- Inputs
 - Problem Management
 - Problem fixes
 - Capacity Management
 - Capacity upgrades
 - Business Relationship Management
 - Customer requests
 - Application Development and Test Lab
 - Application releases
- Outputs
 - Operational Release Management
 - Quality Assurance
 - Configuration Management

Document Maintenance

The Service Integration Management office and associated parties will review the IT Change Management Process document annually for detail and refinement opportunities.

Additional reviews may be conducted as needed to amend policies to reflect changes in **NASA's** IT and business strategies, service offerings, and changing conditions in legal, regulatory, and market conditions. Suggestions or feedback regarding the IT Change Management Process document may be submitted to the document owner, who will formalize and submit draft document revisions for review and approval by the document review board. Once approved, the document owner will update and distribute the document.