2021

CLOUD4C

CHANGE MANAGEMENT PROCESS

ITSM Team
Cloud4C services Pvt Ltd
01-Jan-21

DOCUMENT CONTROL:

PREPARATION

Draft	Author	Date
Version V1.0	Neelash Mansharamani,	23-Feb-16
Version V1.1	Suraj.S	23-Feb-17
Version V2.0	Manish Sakhare	08-May-2018
Version V2.1	Manish Sakhare	1-March-2019
Version V2.2	Manish Sakhare	1-March-2020

REVIEW

Reviewer	Version	Date	Reviewed Draft Version
Ranganathan Govarthanan	V1.0	25-Feb-16	V1.0
Ranganathan Govarthanan	V1.1	23-Feb-17	V1.1
Vishal. M. Reddy	V2.0	08-May-2018	V2.0
Vishal. M. Reddy	V2.1	1-March-2019	V2.1
Vishal. M. Reddy	V2.2	1-March-2020	V2.2
Vishal. M. Reddy	V3.0	1-March-2021	V3.0

TRAINING AND WORKSHOP

Training and Workshop Details	Date
CM Training for all teams	4th March to 7th March 2019
CM Training for all teams	4th March to 7th March 2020

RELEASE

Release Version	Date Released
V2.0	08-May-2018
V2.1	1-March-2019
V2.2	1-March-2020
V3.0	1-March-2021

DISTRIBUTION LIST

Name	Designation	Department
NOC Teams	SM Managers	

CHANGE CONTROL

Version	Change Reason	Effective Date

TABLE OF CONTENTS

INTRODUCTION TO CHANGE MANAGEMENT

Change management is the process responsible for managing the lifecycle of all Changes. ITIL defines 'Change' as a way of handling changes that are agreed, approves and scheduled to ensure the correct level of notification with minimal user impact.

To make an appropriate response to all requests for change requires a considered approach to the assessment of risk and business continuity, change impact, resource requirements, change authorization and especially to the realizable business benefit. This considered approach is essential to maintain the required balance between the need for change and the impact of change.

Change Management process which covers the recording reviewing and authorizing, planning, scheduling, implementation, task creation and reporting of all Change tickets including their relationships to Incidents, Problems and Configuration items etc.

Changes arise due to various reasons:

- Proactively, e.g. seeking business benefits such as reducing costs or improving services or increasing the ease and effectiveness of support
- Reactively as a means of resolving errors and adapting to changing circumstances.

Changes should be managed to:

- Optimize risk exposure (supporting the risk profile required by the business)
- Minimize the severity of any impact and disruption
- Be successful in the first attempt.

KEY DEFINITIONS

CHANGE: The addition, modification or removal of authorized, planned or supported service or service component and its associated documentation.

INITIAL SUPPORT TEAM: The team that provides the very first line of support for processing incidents and service requests. The initial support staff is responsible for resolving incidents at first contact—by identifying known workarounds, using diagnostic scripts, or their domain knowledge.

KNOWN ERROR: An incident or problem for which the root cause is known and a temporary workaround or a permanent alternative has been identified. If a business case exists, an RFC will be raised, but—in any event—it remains a known error unless it is permanently fixed by a change.

MAJOR INCIDENT: An incident with a high impact, or potentially high impact, which requires a response that is above and beyond that is given to normal incidents. Typically, these incidents require cross-company coordination, management escalation, the mobilization of additional resources, and increased communications.

PROBLEM: The undiagnosed root cause of one or more incidents.

SUPPORT/KEY SUPPORT: A function that provides the vital day-to-day contact point between customers, users, IT services, and third-party organizations. The Support/Key Support team not only coordinates the incident management process but also provides an interface into many other IT processes.

SERVICE REQUEST: Any demand from User placed upon IT. Requests are handled & managed by Request Fulfilment process

SOLUTION OR RESOLUTION: Also known as a permanent fix. An identified means of resolving an incident or problem that provides a resolution of the underlying cause.

WORKAROUND: An identified means of resolving a particular incident, which allows normal service to be resumed, but does not resolve the underlying cause that led to the incident in the first place.

PURPOSE & OBJECTIVES

PURPOSE

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

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

OBJECTIVE

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

SCOPE

The scope of Change Management covers changes to baseline service assets and configuration items across the whole service lifecycle. Each organization should define the changes that lie outside the scope of their service change process. Typically these might include:

- Changes with significantly wider impacts than service changes, e.g. departmental organization, policies, and business operations – these changes would produce RFCs to generate consequential service changes.
- Changes at an operational level such as repair to printers or other routine service components.

VALUE TO THE BUSINESS

Reliability and business continuity are essential for the success and survival of any organization. Service and infrastructure changes can have a negative impact on the business through service disruption and delay in identifying business requirements, but Change Management enables the service provider to add value to the business by:

- Prioritizing and responding to business and customer change proposals.
- Implementing changes that meet the customers' agreed service requirements while optimizing costs.
- Contributing to meet governance, legal, contractual and regulatory requirements.
- Reducing failed changes and therefore service disruption, defects and re-work.
- Delivering change promptly to meet business timescales.
- Tracking changes through the service lifecycle and to the assets of its customers.
- Contributing to better estimations of the quality, time and cost of change.
- Assessing the risks associated with the transition of services (introduction or disposal).
- Aiding productivity of staff through minimizing disruptions due to high levels of unplanned or 'emergency' change and hence maximizing service availability.
- Reducing the Mean Time to Restore Service (MTRS), via quicker and more successful implementations of corrective changes.
- Liaising with the business change process to identify opportunities for business improvement.

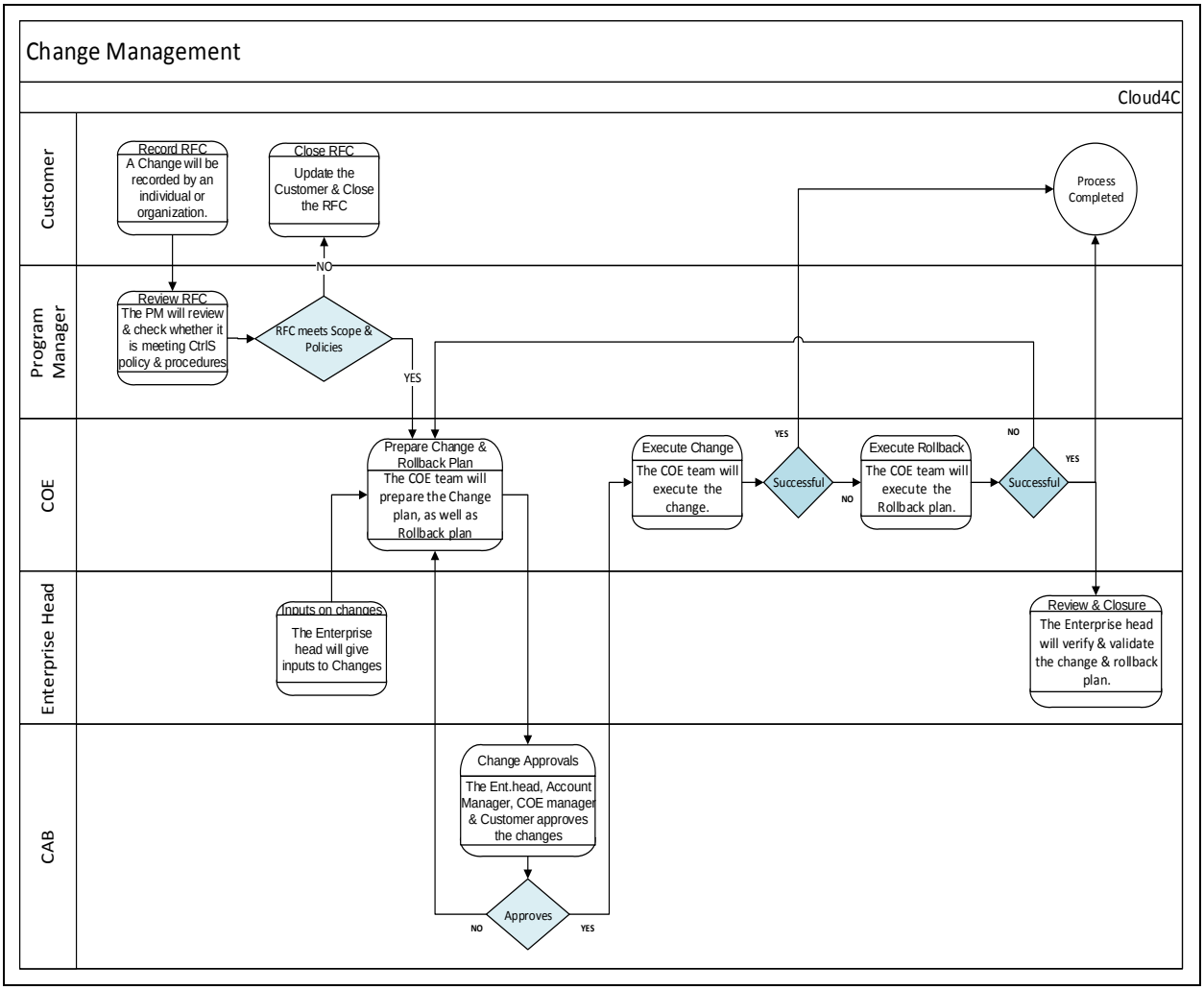
POLICIES

Policies that support Change Management include:

- Creating a culture of Change Management across the organization where there is zero-tolerance for unauthorized change.
- Prioritization of change, e.g. innovation vs. preventive vs. detective vs. corrective change.
- Establishing accountability and responsibilities for changes through the service lifecycle.
- Segregation of duty controls.
- Establishing a single focal point for changes to minimize the probability of conflicting changes and potential disruption to the production environment.
- Preventing people who are not authorized to make a change from having access to the production environment.
- Integration with other Service Management processes to establish traceability of change, detect unauthorized change and identify change related incidents.
- Change windows – enforcement and authorization for exceptions.
- Performance and risk evaluation of all changes that impact service capability.
- Performance measures for the process, e.g. efficiency and effectiveness.

PROCESS OVERVIEW

OVERVIEW OF PROCESS ACTIVITIES



TRIGGERS, INPUT & OUTPUT

TRIGGERS

• The procedure begins when a Request for Change (RFC) is initiated. All members of CtrlS and authorized customers can submit an RFC.

INPUTS

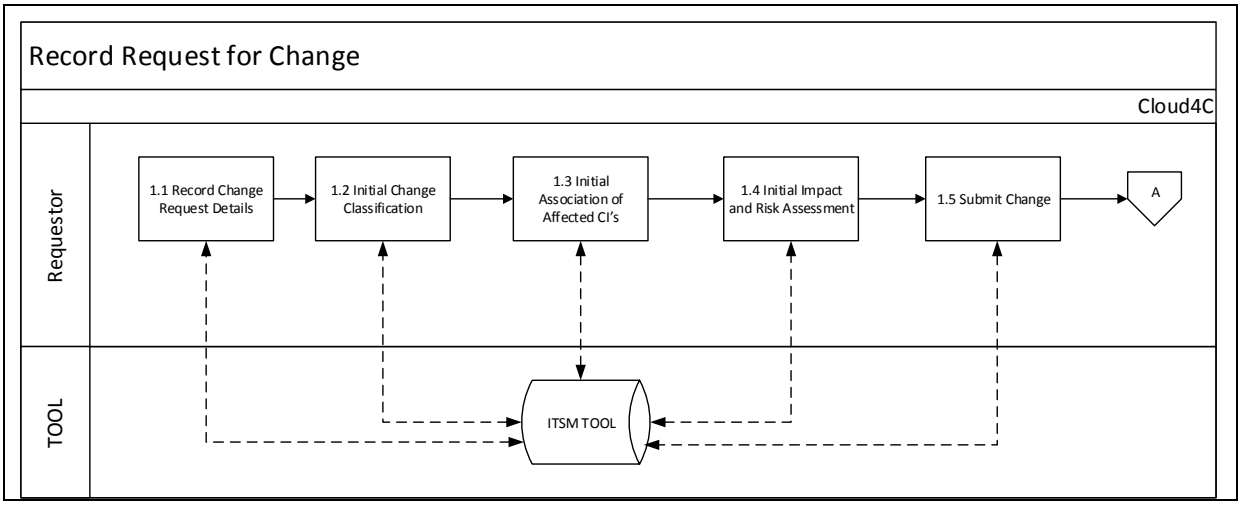
- Requests for Change
- Emergency Changes to resolve Incidents and restore service
- Configuration Management – Configuration Item information available to Change Management.
- Capacity information
- Availability information
- Solution to Problems resolved through problem management process
- Approved Service Requests
- Configuration details from the CMDB
- Incidents
- Known Errors
- Projects
- Releases
- Service level management
- Event management
- Assets and configuration management

OUTPUTS

- Approved and scheduled Change Requests
- Forward Schedule of Change
- Change reports
- CAB minutes and actions
- Rejected Changes with proper justification
- Completed RFCs
- Change Advisory Board schedules
- Post Implementation Review

PROCEDURES

RECORD REQUEST FOR CHANGE



1.1 Record Change Details

A change will be recorded by a request from an individual or organization that required the change. Major changes, such as those which have a significant impact in terms of cost or organizational change, will require an appropriately signed off change proposal, which will contain a full Definition of the change and business and financial justification for the proposed change. Requests for change will be logged by authorized change requesters.

1.2 Initial Change Classification

There are two types of classification. They are Operational Categorization and Product Categorization. Operational and Product Categorization are required to be completed during the creation of a Change.

Operational Categorization Guidelines:

Tiers	Definition
Tier 1	Adjective of what is being done or performed Example: Install, upgrade, configure
Tier 2	High-level component that is being affected

Product Categorization Guidelines:

When selecting the Product categorization, if you know the name of the product or service that is affected, you can go directly to Tier 3 and select the appropriate entry. These will backfill the options for Tiers 1 and 2.

Tiers	Definition
Tier 1	High-level organization of products and services Example: Infrastructure = Server, Database, network
Tier 2	Mid-level break-down of products and services
Tiers	**Definition**
Product Name	Name of the product or service Example: Outlook or Lotus Notes
Model/Version	Specific version of the product name Example: Outlook 2000

1.3 Initial Association of Affected CI's

Relate any Configuration items that would be impacted or changed or their associated dependencies in the change ticket/request for change.

1.4 Initial Impact and Risk Assessment

Every change has an associated risk. The person who requests the change should assess the risk level of the change. Modelling the change in environmental conditions can also help assess the risk of a change. The recommendation is to assign one of these risk categories to each change request and also answering the 7 R's of change.

Implementing a Change is introducing a corrective measure – either as rectification of an existing Configuration Item (CI) or an introduction of an entirely new CI – to a business environment. And as every component/CI works in sync with the other CIs, they create and maintain a certain balance among themselves in the environment. A new introduction/Change can upset this balance posing a risk to the other CIs and, by extension, to the organization.

Risk Assessment

It is an exercise to minimize this risk, helping the organization to assess the risk it will bear as a result of a Change Implementation. It is an assessment of technical and business aspects of a Change affecting, for example, hardware, software, network, feasibility, etc.

Seven R's questionnaire:

- Who raised/requested the change?
- What is the reason for the change?
- What is the return required from the change?
- What are the risks involved in the change?
- What resources are required to deliver the change?
- Who is responsible for the build, test and implementation of the change?
- What is the relationship between this change and other changes

Impact and Urgency:

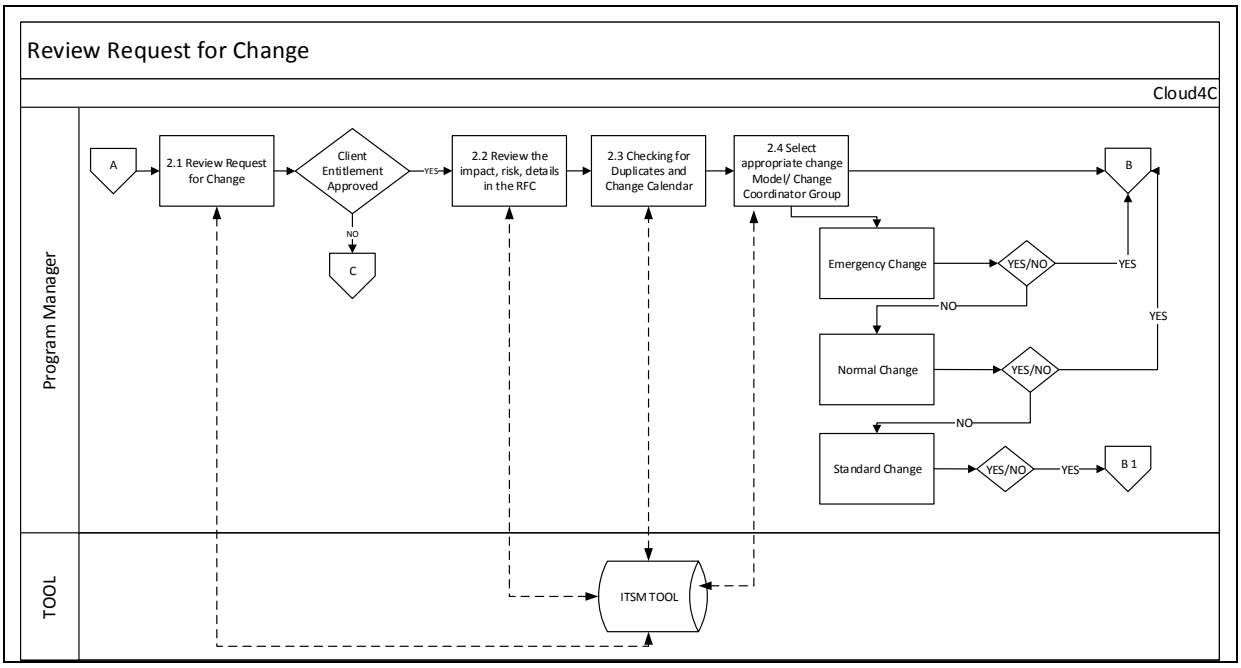
Business impact is the planned impact of a Change, and the aggregate effect it will have on a client's business when it is implemented into the target environment.

To what extent an Incident results in a deviation from the normal service level; aspects are the number of users, Infrastructure and the service concerned/affected.

1.5Submit Change: The Requester has to submit a change in the Service Delivery tool with the above mentioned details filled in. In case of any Clarifications/Queries on the Submission of change, the Requester can always consult the change Manager.

REVIEW REQUEST FOR CHANGE

The program manager will review and check whether it is meeting the CtrlS defined policy and procedures.



2.1 Review Request for change: Program Manager reviews RFC for accuracy of information provided by the Requester, Check if the Request is in scope. Upon receipt of a Request for Change, the Program Manager will perform the following:

- Validate that the client is entitled to the Change services.
- Validate that the Change meets all of the CtrlS process criteria.
- All the necessary information is present to begin planning activities

2.2 Review the Risk, Impact Details in the RFC: Program Manager will review the Risk and Impact details for the second time to identify the correct classification and Change class/Model/timings. In case some information is missing the Program manager contacts the Requester for further information.

2.3 Check for Duplicates and Change Calendar: Another responsibility of Program Manager is to ensure that they are no duplicate changes which have been processed in the past and check for any other changes which are to be carried out on this CI, if so then plan things according to the availability. Program Manager Checks for Duplicates requests and either would associate them or inform the Requester and cancel the change ticket.

2.4 Select appropriate change model and Change Coordinator Group: Program Models/Class/timings are selected based on the lead times, Risk and Urgency of the change. CtrlS

has three models of changes which can accommodate any type of request for change from the Customer

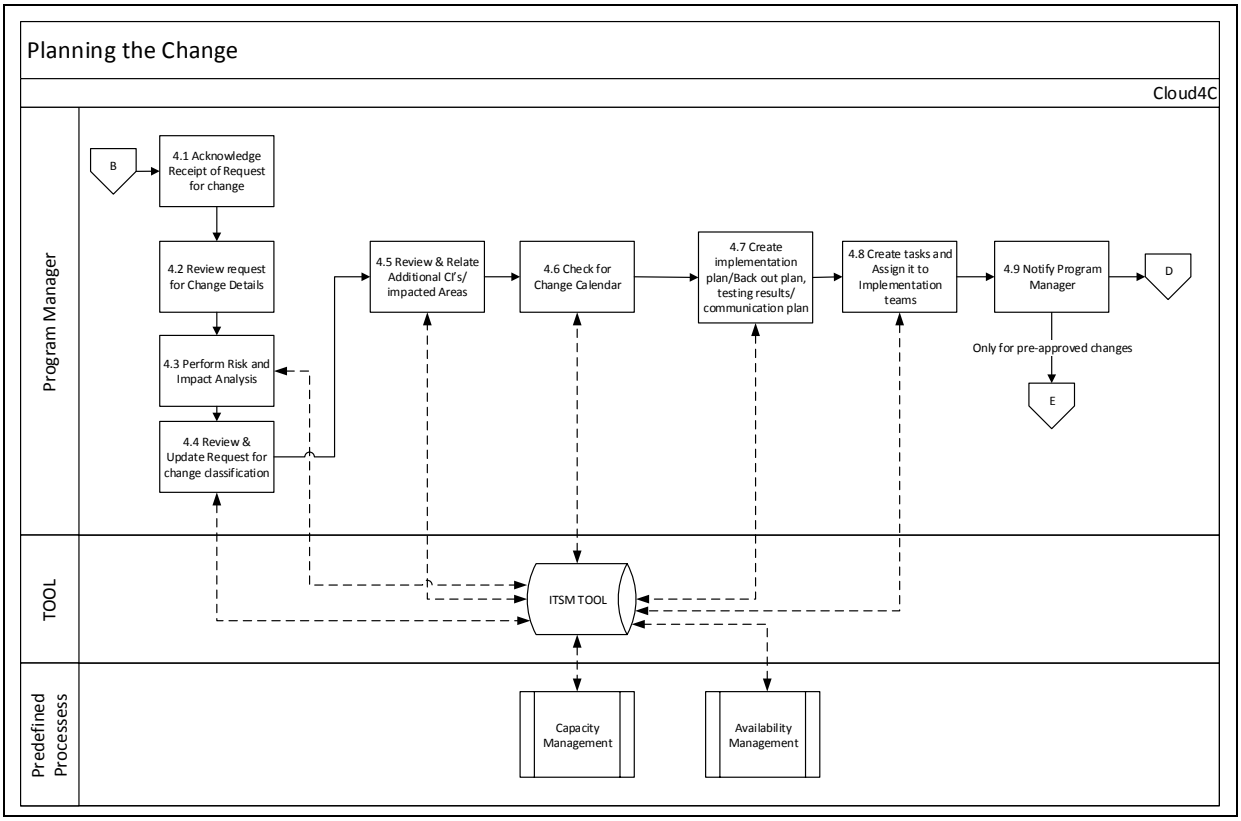
B1 Standard Changes: Pre-Approved changes are typically pre-approved and require no CAB approvals. However, a business level approval would be mandatory. These changes are low risk, low impact with High frequency changes.

B Normal Changes: A change that requires Change Management approval, and encompasses the majority of changes which carry High Risk, High impact.

B Emergency Changes: In response to a Priority 1 or Priority 2 Production incident. To resolve/ restore service.

PLANNING THE CHANGE

Change planning is the process of planning a change that includes the identification of requirements, ordering of required hardware and software parts, checking power budgets, identification of human resources, creation of change documentation, and the review of technical aspects of the change and change process.



4.1 Acknowledge the Receipt of Request for Change: After having been assigned a new Request for Change, the COE engineer reviews the request details to make sure they have a clear understanding of what is being requested, and acknowledges the RFC.

4.2 Review Request for Change Details: Review details provided by the Requester and identify the required resources, planning, testing, effort and financial requirements if any for the change.

4.3 Perform Risk and Impact Analysis: COE engineer performs the Risk and impacts analysis for the third time in change lifecycle. Every change has an associated risk. The person who requests the change should assess the risk level of the change. Modelling/testing the change in a test environment will help assess the risk of a change. The recommendations and impact can be clearly defined and Implementation plans can be built as per the testing results. Update the Risk level and impact level in case we have any changes to change ticket.

4.4 Review and update Request for Change Classification: Review and update the any Change classifications indicated in the Change.

4.5 Review and Relate Additional CI's/Impacted Areas: Once the Risk and Classification is reviewed and updated COE Engineer relates any additional Configurations items and the Impacted areas.

4.6 Check for Change Calendar: Check for any conflicts with other changes that are planned through change calendar and determine outage that is required for the change with the help of Availability plan (Incase Availability and Capacity Management is in scope). Forward schedule

change checking what is the best time to implement the change in sync with Capacity management.

Program manager coordinates the change schedule across to production. Changes will be scheduled to meet the business need. By agreement with the customer, change and release windows will be established, to assist in the planning of changes and releases and the numbers of each that can be implemented.

4.7 Create Implementation Plan/Back-out plan, Testing Results/Communication Plan: Carefully planning of the change will ensure that there is no ambiguity about the requests included in the change Management process, tasks included in other Processes and how they interface with other suppliers or Projects. COE engineer should plan the schedule changes to meet business rather than IT needs.

The COE engineer will ensure that all access, documentation, plans, hardware, software, networking and human resources required to implement the change are available. He will check that the personnel involved have the required skill-set and experience and have the appropriate security clearance.

Test plans will be created and validated for the change to ensure that once the change has been implemented the success of the change can be tested.

CI's are to be prepared and tested in preparation for implementation into the production-computing environment. Pre-implementation testing is performed on all change build activity. The results are validated and documented for review by the Technical Manager.

Each change will be tested in preparation for implementation and results stored in the change record.

Prepare a backout plan in case the change does not go as per plan, what are the steps that should be taken to ensure that services are back up and running within specific time frame and with less impact. For Major impact changes, this can be developed with the help of IT continuity service management.

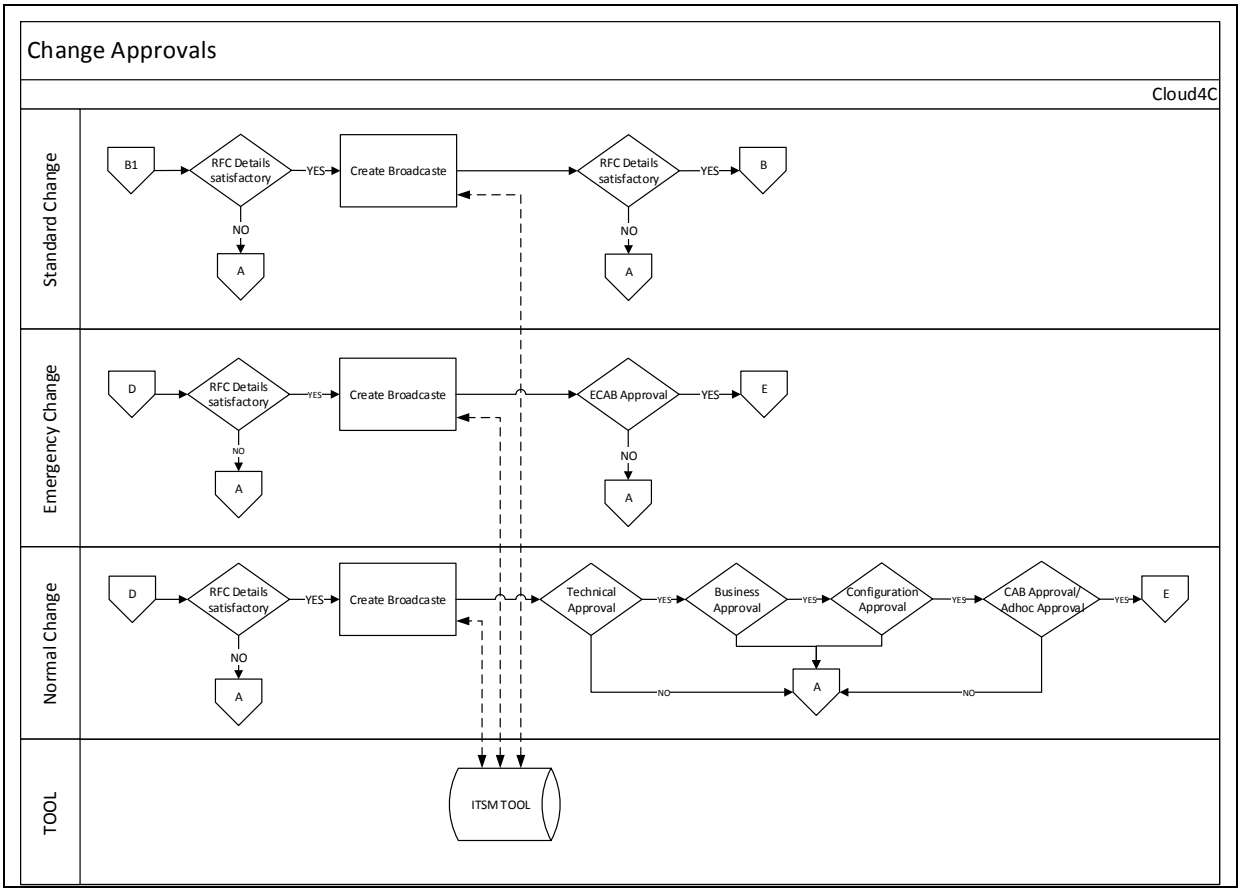
The Program manager and COE Engineer take the responsibility to ensure that communication to relevant groups.

4.8 Create tasks and Assign it to Implementation teams: Create tasks and assignments depending upon type and impact of the change. Changes need to be assessed for their Hardware & Software requirements. Human resources are confirmed to be available to implement and support the change. Assessment should also be given to the on-going Capacity requirements of the change. Hence Tasks and assignments are created to ensure the responsibility of the changes.

4.9 Notify Program Manager: Once the Request for Change has gone through the Planning phase, the COE engineer will inform the Program Manager to initiate the collection of the necessary approvals.

CHANGE APPROVALS

The CR owner will review the Change plans and all associated documentation prior to engaging the approval process. If they have any questions, they will contact the Change coordinator to gather additional information or documentation.



(B1) Standard Change Approval: Selecting the appropriate change model: a single business approval i.e. Resolve ticket or mail is required for Standard/no Impact change, a Broadcast is created to notify the Approval and business as per Communication plan. If the Change is not in conflict with any internal standards or policies, the CR owner determines if there is a business approval required.

If a business approval is required, the system will kick off the approval request to the required business approver. If there is no business approver already set up in the system, the CR owner will need to set up an ad-hoc business approval.

Once the approval is received, the CR owner will assign a COE engineer and update the Change to indicate planning is in progress. If the Standard Change Request is not approved by the business approvers, the CR owner will reject the Change and notify the Change Requester of the Change rejection.

If a business approval is not required, the CR owner will assign a COE engineer and update the Change to indicate planning is in progress.

(D) Emergency Change Approval: Selecting the appropriate change model, business approval i.e Resolve ticket or mail & ECAB approval is required for Emergency Change. After a COE Engineer & CR owner have informed the COE manager that an Emergency Change is required to

be executed, the COE manager reviews the Change & along with Program manager presents the Change for ECAB approval. If the ECAB finds the Change to be in conflict with any internal Change standards or policies, he/she informs the COE engineer that the Change cannot be implemented.

If the Change is not in conflict with any internal Change standards or policies, the CR owner reviews the Change plan information including risk assessment and the Implementation Plan. The Program Manager checks the plan to ensure that appropriate precautions have been planned to minimize both the risk of failure and the impact on the user(s)/ services, and that the timing of the implementation does not conflict with other planned Changes or planned events.

If the Change plan is found to be insufficient, the ECAB requests additional analysis from the COE engineer. Similarly, if the planning does not adequately address the risk of failure or the impact on the user(s)/services, or if the planning conflicts with other planned Changes or events, the ECAB requests an adjustment of the Implementation Plan from the COE engineer.

On the other hand, if the planning of the implementation appears to be in order, the CR owner ensures that the necessary approvals will be collected for the Change.

Approval level required for an Emergency Change is:

Emergency Change Advisory Board (ECAB): Not all Emergency Changes have to go through a formal ECAB approval. If the Emergency Change is in response to a Priority 1 or Priority 2 Incident in progress and the Emergency Change is to restore service, the Emergency Change can be completed as needed.

If the Change is rejected by the ECAB, the CR owner will determine why it was rejected and will ask the COE engineer to make the required modifications to the planning documents. This may include performing additional Risk & Impact Analysis or to adjusting the planning if that was the reason why the Change was rejected. If the Change plan cannot be modified to address the issues identified in the rejected Change, the CR owner informs the COE engineer that the Change cannot be implemented and the Change is cancelled.

(D) Normal/Expedited Change Approval: Selecting the appropriate change model, business approval i.e. Resolve ticket or mail, CAB approval & COE manager approval is required for Normal Change. After a COE engineer has informed the Program Manager that a Change is ready for approval, the Program Manager reviews the Change. If the CR owner finds the Change to conflict with any internal Change standards or policies, he/she informs the COE engineer that the Change cannot be presented in the CAB for approval.

If the Change is not in conflict with any internal Change standards or policies, the CR owner reviews the Change plan information including risk assessment and the Implementation Plan. The Program Manager checks the plan to ensure that appropriate precautions have been planned to minimize both the risk of failure and the impact on the user(s)/services, and that the timing of the implementation does not conflict with other planned Changes or planned events.

If the Change plan presented by Program Manager is found to be insufficient, the CAB requests additional analysis from the COE engineer Similarly, if the planning does not adequately address the risk of failure or the impact on the user(s)/services or if the planning conflicts with other planned Changes or events, the CAB requests an adjustment of the Implementation Plan from the COE engineer.

On the other hand, if the planning of the implementation appears to be in order, the CR owner ensures that the necessary approvals will be collected for the Change.

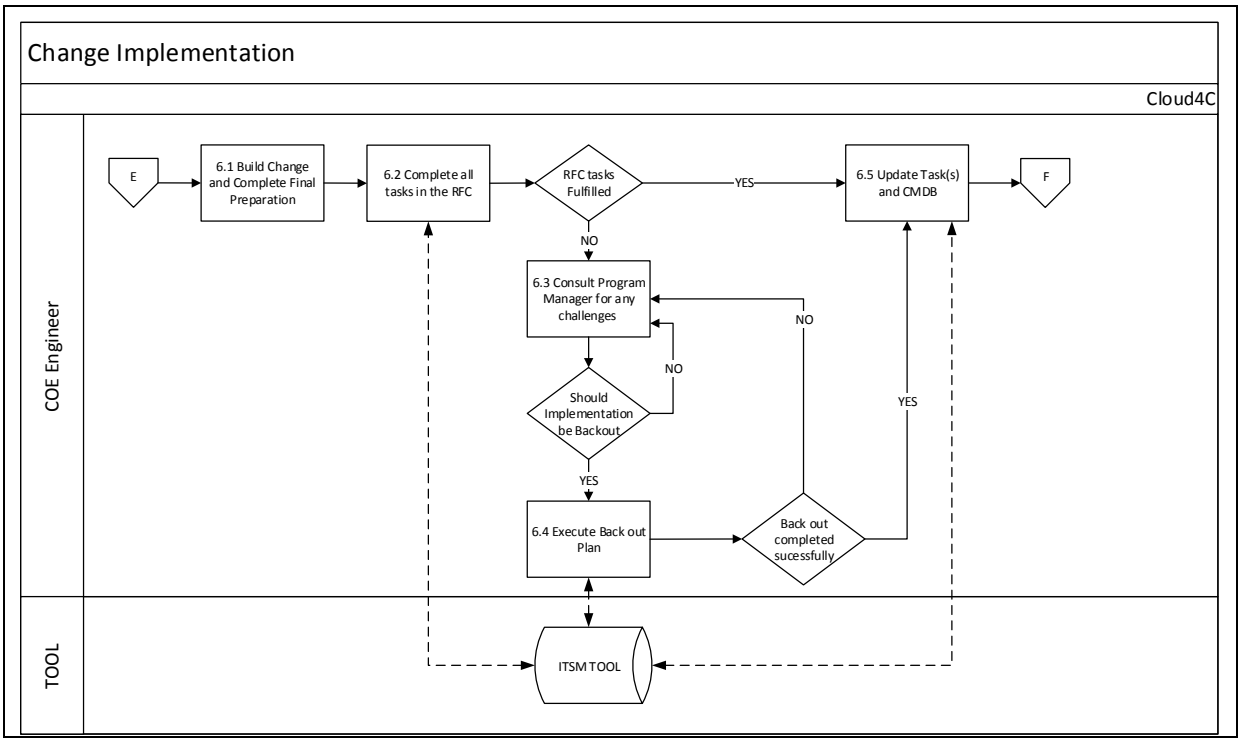
Approval levels required for a Normal Change are:

- Technical Approval of Change

- Business Approval of Change
- Configuration manager approval
- Adhoc approvals
- CAB approvals

CHANGE IMPLEMENTATION

This procedure is used to implement planned and approved Changes. The COE engineer will use the Change Implementation and Test Plans to implement the planned and approved Change. The COE engineer will use the Back-out Plan (as needed) to back out the intended Change implementation.



(6.1) Build change and complete final preparation: After the Change has been approved; the first implementation task(s) of the Change is ready to begin implementation at the scheduled time. The COE engineer first prepares for the implementation (i.e., to ensure operational readiness). This can involve performing system backups, performing tests, making sure tools and resources are available, etc.

(6.2) Complete all tasks in the RFC: When everything is ready, the COE engineer completes the task(s) for the actual implementation of the Change. They identify if requirements of the Change Task were fulfilled and if the implementation of the Back-out Plan is needed. In case of a service outage or when the Changes are extending the window and significant impact is observed, inform Program manager and get an incident created for the same.

(6.3) Consult Program Manager for any Challenges: Escalate to the Change Coordinator any change which is not going according to plan. After the Change has been put into production, a Level 2 or 3 (with the help of a user if the Level 2 or 3 does not have sufficient access rights) performs the production test to verify the success of the implementation. In case of any challenges during implementation, the Task implementer consults Change coordinator for challenges and results after implementation is communicated back to the Change Coordinator and Change Manager

If all Change requirements have not been fulfilled, however, Level 2 or 3 who performed the production test determines if the Change implementation should be backed out. Change is backed out if its implementation does not provide an improvement over the previous situation, or causes a security or data integrity risk.

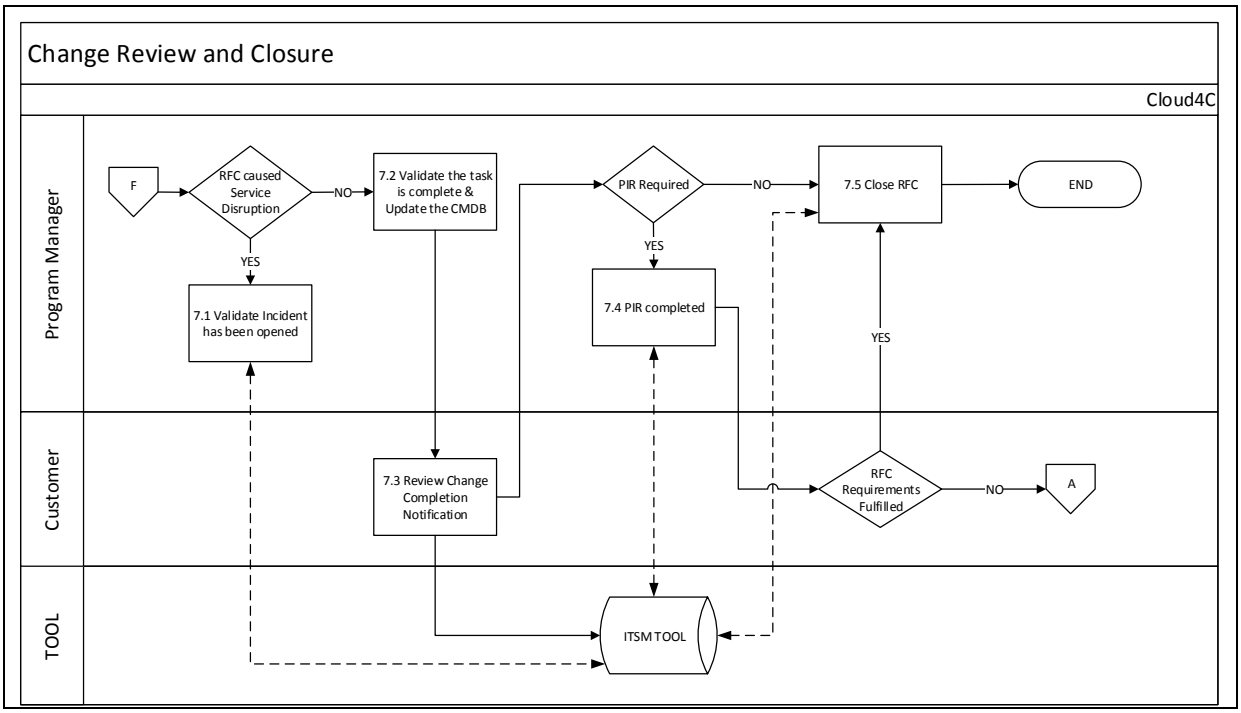
(6.4) Execute Back-out plan: If the back-out of the current implementation is required, the COE engineer would notify the Program Manager that the Back-out Plan will need to be executed and will then execute the Back-out Plan and verify the success of the back-out.

(6.5) Update Task(s) and CMDB: Record in a timely manner the start and finish dates/times of the change. Once all of the task implementation activities have been performed, the engineer will update their respective Task record to notify the Program Manager that the Change Tasks have been completed.

Once the RFC has been implemented and verified as successful the COE engineer will be responsible for updating the CI in the CMDB to reflect any variance resulting from the RFC.

CHANGE REVIEW AND CLOSURE

This procedure is used to close the Change Tasks after the planned Changes have been implemented and by Program Manager to close the Change Request after they have validated that the Change has been completed. It is also used by the Requester to view the completeness of the Change Requests.



(7.1) Validate incident has been opened: In case of an Outage or a change which was not processed as per the Implementation plan, or when the back-out plan was implemented, ensure that an Incident record is created. Program Manager ensures the same.

(7.2) Validate the task(s) is completed and CMDB is updated: Validate if tasks are implemented correctly, the scheduled time mentioned is correct. Also, Validate if the communication about updates (if any) was passed on to the Configuration manager.

(7.3)Review Change Completion Notification: The Engineer responsible for change implementation will work with the Program Manager to collate all the information (results and documentation associated with the change) and make it available for review.

The Program Manager will review the completed change to establish that the Change Requester, Sponsors and customers are content with the results and identify any shortcomings. Also the review will assess whether the change was implemented on time and inside the budget.

(7.4) PIR Completed: A Post Implementation Review (PIR) will be performed on the failed change requests.

The PIR will be conducted and documented by the CR owner within 48 business hours of the completion of the Change. The PIR will be presented to the CAB at the next available CAB meeting.

A PIR is performed to identify:

- Lessons learned to prevent future implementation issues or Incidents
- Technical Success of the Change
- Unwanted or Undesirable Side Effects
- Effectiveness
- User Satisfaction

(7.5) Close RFC: Once the change has passed through the verification period successfully then the Program Manager will ensure that the CI in the CMDB has been updated to reflect the outcome of the change and placed in the status of "Approved" and the change and RFC will be formally closed by the Program Manager. This will trigger an approved baseline status for the CI.

If the Change is completed as requested, but there were no issues raised, the Program Manager will validate that all Tasks have been completed and will have all the necessary information for closure.

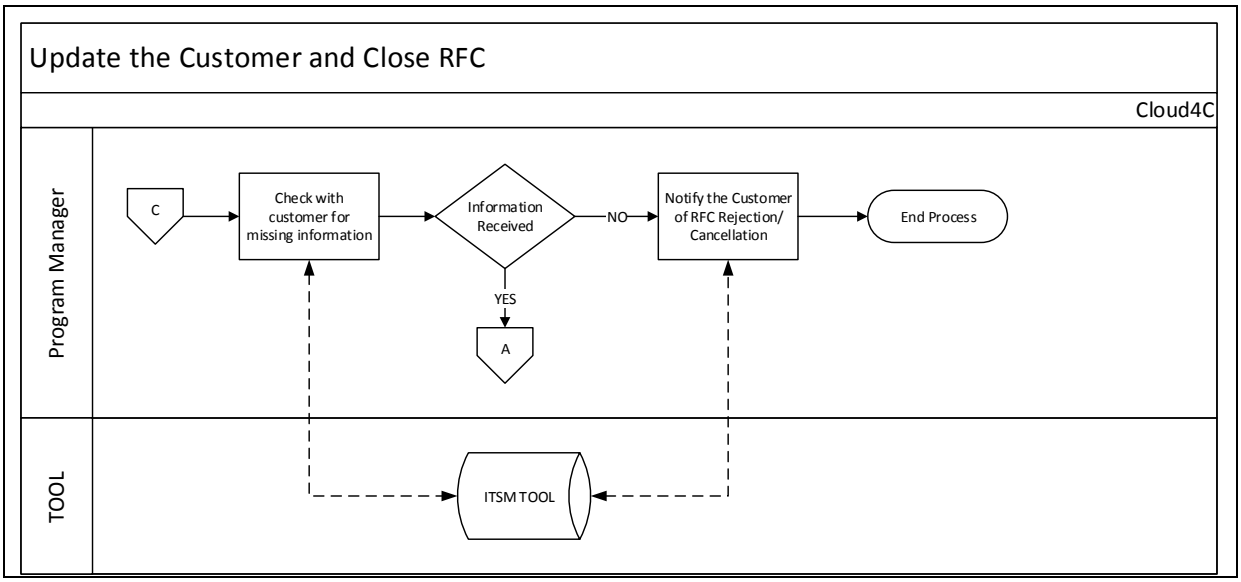
After all, Tasks have been updated and closed, the Program Manager closes the Change.

The Program Manager finally ensures that the Requester and approvers of the Change are informed that the Change has been completed.

After the Program Manager closes the Change, the Requester will receive notification that the Change has been completed. The Requester can then check whether his/her requirements have been fulfilled. If the Requester has verified that the requirements have been met, he/she does not need to take any action.

UPDATE THE REQUESTER AND CLOSE RFC

This is at the stage where incomplete and inaccurate data is provided by the requester



(C) Incase Output for any task is C it requires additional information or information is missing.

Program Manager Checks for more information from the Requester, once the information is received it is fed in the change ticket and the process restarts.

Incase due to what so ever reason or business justification or risk or the scope of the change is not provided to Program manager, the Requester is notified that the change is set to cancelled status.

KEY PERFORMANCE INDICATOR'S

KPI	Definition	Frequency	Unit
Successful Changes	Increase in the number of Changes that have been closed successfully, divided by the total number of closed Changes.	Monthly	% of Changes
Emergency Changes	Reduction in the number of completed Changes with a Change timing of Emergency.	Monthly	% of Changes
Time to plan	The average time it takes, from the moment a Change has been registered, until it's ready for approval.	Monthly	% of work hours
Time to approve	Reduction in the average time it takes for a Change to gain approval.	Monthly	% of work hours
Backlog of Changes	The number of Changes that are still in process and have not been completed.	Daily	% of Changes
Service Impacting changes	The Number of changes that resulted in Outages due to incorrect planning, delays	Monthly	% of Changes

CHANGE MANAGEMENT ROLES & RESPONSIBILITIES

Responsibility	Customer	Program/ Project Manager	CAB/ Approvers	COE Engineer /Team	Quality Head/ Delivery Head	CRM
States the benefit of a Change Request in relation to its cost, benefit and risk.	C/I	R/A	R	C	I	
Ensures that conflicts are avoided and schedules are maintained at a manageable level.	C	R/A	C/I	C/I	I	
Manages CAB Meetings.	I	R/A	R	I	I	
Publishes agreed Changes to the FSC*. *FSC – Forward Scheduled Changes	I	R/A	C	C/I	I	
Provides reports on schedule.	I	R/A	I	R	I	
Prioritizes and escalates all Changes in accordance with the classification matrix and service levels.	C	R/A	C/I	C/I	I	
Manages Emergency and Fast Track Changes.	I	R/A	R	R	I	
Approve Latent Change.					R/A	R/A
Ensures that all implementation and approval lead times are adhered to and exemptions correctly managed.	R	R/A	R	R	I	
Provides feedback on issues to facilitate improvements.	R	R/A	R	R	I	
Schedules Change and business testers (if required).	C	R/A	C	C	I	

Responsibility	Customer	Program/ Project Manager	CAB/ Approvers	COE Engineer /Team	Quality Head/ Delivery Head	CRM
Change Initiation						
Creates Change record and attaches SOW and other required items within agreed lead times.	R	A/R	I	R	I	
Assigns Technical Assessment tasks.	I	A/R	I	C/I	I	
Raise a Latent Change						R/A
Technical Assessment						
Completes technical assessment; completes SOW; escalates issues as required.	C	R/C/I	I	A	I	
Liaises with the Requester for scope, impact, schedule and resource issues.	C	A/R	C	C	I	
Reviews security-related Change components; rejects if any compliance issues are identified.	I	R/A	C	I	I	
Accepts/rejects/queries Change.	I/C	R	A/R		I	
Assigns rejected Changes back to the technical assessor(s) with feedback.	C	A/C	C	I	I	
Implementation						
Accepts and prepares for Change and ensures it is on schedule.	C/I	R/C	C	A/R	I	
Initiates only as scheduled; follows implementation instructions precisely.	C/I	C/I	I	A/R	I	

Responsibility	Customer	Program/ Project Manager	CAB/ Approvers	COE Engineer /Team	Quality Head/ Delivery Head	CRM
Confirms Change success with the Implementation Tester.	I	C/I	I	A/R	I	
In the event of implementation failure, escalates as required for decision re: back out.	C	C/R	I	A/R	I	
Ensures that records are updated and completed as soon as the Change has been implemented or backed-out.	I	I/A	I	R	I	
Change Review and Closure						
Ensures that Post Implementation Reviews are completed on schedule.	I	R/A	C	R	I	
Closes Change record as agreed with Initiator.	C	R/A	I	R	I	
Change trending analysis	I	R/A	I	C	I	

INTERFACE WITH OTHER PROCESSES

Other Process	Input provided to Change Management	Outputs received from Change Management
Incident Management	• Emergency change	• Restoration of services by executing emergency change
Problem Management	• Known Errors • Permanent fixes after root cause analysis	• Fixing known errors/ Permanent fixes through Change management process

KEY PERFORMANCE INDICATOR & PROCESS MEASURES

Achievement against KPIs should be monitored and used to identify opportunities for improvement Each CSF is followed by certain KPI's which supports that CSF.

Following are the KPI's of Change Management Process:

- The number of changes implemented to services which met the customer's agreed requirements.
- The benefits of change expressed as 'value of improvements made' + 'negative impacts prevented or terminated' compared with the costs of the change process
- Reduction in the number of disruptions to services, defects and re-work caused by inaccurate specification, poor or incomplete impact assessment
- Reduction in the number of unauthorized changes
- Reduction in the backlog of change requests
- Reduction in the number and percentage of unplanned changes and emergency fixes
- Change success rate (percentage of changes deemed successful at review/number of RFCs approved)
- Reduction in the number of changes where remediation is invoked
- Reduction in the number of failed changes
- Average time to implement based on urgency/priority/change type
- Incidents attributable to changes
- Percentage accuracy in change estimate.

Output measures

- Number of disruptions, incidents, problems/errors caused by unsuccessful changes and releases
- Inaccurate change specifications.
- Incomplete impact assessment
- Unauthorized business/customer change by business/IT/customer/user asset or configuration item type.
- Percentage reduction in time, effort, cost to make changes and releases.
- Service or application re-work caused by inadequate change specification
- Percentage improvement in predictions for time, quality, cost, risk, resource and commercial impact
- Percentage improvement in impact analysis and scheduling of changes safely, efficiently and effectively reduces the risk of changes affecting the live environment
- Percentage reduction in unauthorized changes.

Workloads

- Frequency of change.
- Volume of change.

Process measures

- People's satisfaction with the speed, clarity, ease of use
- Number and percentage of changes that follow formal Change Management procedures