Change Management

change management Process

**Supplemental to Information Technology Corporate Standard (ITCS) 104, Chapter 1, Section 1.6 Activity Auditing, Requirements 1, 2, and 3**

© 2013-2017 IBM. All Rights Reserved.

Revision History

| version | Date | APPROVED BY | Description of the Change |
| --- | --- | --- | --- |
| 0.1 | 20-Sep-2007 | Kay Lipps | Initial Draft |
| 0.2 | 15-Jan-2013 | Kay Lipps | Integrated Verizon-acquired services into Terremark Change Management process. |
| 0.3 | 13-Jun-2013 | Giacomo Deannuntis, Art Griffin | Format/edit v0.1 – v0.2. Spell/grammar checks OK. |
| 0.4 | 13-Jun-2013 | Kay Lipps | Reviewed and updated all Hyperlinks. |
| 0.5 | 21-Jun-2013 | Art Griffin | Deleted “Terremark Worldwide, Inc.” from the cover page. Corrected the Terremark URL. Inserted new Copyright text. Changed “Terremark” to “Verizon Terremark.” Cross-checked all Definitions and deleted Definitions table. |
| 0.6 | 26-Jun-2013 | Kay Lipps | Updated document publication date. |
| 0.7 | 26-Jun-2013 | Art Griffin | Format/edit v0.6. Accept all changes per document owner. Spell/grammar checks OK. |
| 1.0 | 26-Jun-2013 | Art Griffin | Received owner approval. Change v0.7 to v1.0. Delete Draft watermark. PDF and post to TMQM SP. |
| 1.1 | 19-Jun-2014 | Paul Hsia | Adding flowchart in Appendix A. |
| 2.0 | 27-Jun-2014 | Kay Lipps | Approved version. |
| 2.1 | 06-Nov-2015 | Kay Lipps | Annual review and updates. Added RACI, Measures. |
| 2.2 | 13-Nov-2015 |  | Reviewed by policy analyst (Y. Dumas); additional recipients provided by P. Hsia added to the Distribution List |
| 3.0 | 30-Nov-2015 | TCC | Approved for publishing |
| 3.1 | 29-Feb-216 | Paul Hsia | Added section 16; updated section 5 detailed implementation steps, Section 10 TRM & Appendix B. The content reviewed by Nathan Sutton (Lifecycle A7E Support – Problem Management) and Jon Bolduc on behalf of Shannon Soland (Lifecycle A&E Support – Incident Management)  The changes reflect improvements suggested during SSAE 16 audit. |
| 3.2 | 29-Feb-2016 |  | Policy Management Review and Approval for TCC Review. Document will require TCC and CISC Approval. |
| 3.3 | 21-Mar-2016 | TCC | Approved by TCC; per TCC review a note added to Service Request for Section 16 |
| 3.4 | 07-Apr-2016 | CISC | Approved by CISC (4/1); one minor change to add audit information was completed (see Document history entry 3.1) |
| 4.0 | 08-Apr-2016 | Kay Lipps | Approved for publishing |
| 4.1 | 26-Jan-2017 |  | Updated section 7 to add the word ‘network’ - “Dedicated Customer Environment (DCE) changes for dedicated customer *network* gear” |
| 4.2 | 31-Jan-2017 |  | Change ECME environment notification tool to “Outage Notification” |
| 4.3 | 03-Feb-2017 |  | Minor formatting updates |
| 4.4 | 28-Feb-2017 |  | Policy Management Review TCC Schedule March 6, 2017 |
| 5.0 | 06-Mar-2017 | TCC | TCC Approved for Publishing |
| 5.1 | 12-Oct-2017 |  | Checkout for updates, template updated |
| 5.2 | 17-Oct-2017 |  | Policy Management Review |
| 5.3 | 30-Oct-2017 |  | SME Updates and Policy Management Review of Changes:   * Appendix D Distro list still needs to be updates to IBM Email distros. * Section 10 email addresses need to be updated to GCTS/IBM email distros |
| 5.4 | 6-Nov-2017 |  | TCC Review; pulled from TCC review by R. Hawkins for additional changes |
| 5.5 | 13-Dec-2017 |  | Ready for TCC review (NOTE: it needs email distribution address for S. Soland’s organization) |
| 5.6 | 18-Dec-2017 | TCC | TCC Review and Approval for Publishing |

Table of Contents

[1 Process Overview 1](#_Toc497286181)

[1.1 Purpose 1](#_Toc497286182)

[1.2 Scope 1](#_Toc497286183)

[1.3 Alignment with Corporate Policies 2](#_Toc497286184)

[2 Change Management Phases 3](#_Toc497286185)

[3 Roles and Responsibilities 4](#_Toc497286186)

[3.1 Requestor 4](#_Toc497286187)

[3.2 Peer Reviewer 4](#_Toc497286188)

[3.3 Change Administrator 5](#_Toc497286189)

[3.4 Change Executor 5](#_Toc497286190)

[3.5 Change Advisory Board 6](#_Toc497286191)

[3.6 Executive Review Board 6](#_Toc497286192)

[3.7 CAB Executive Committee 6](#_Toc497286193)

[3.8 Tactical Response Manager 7](#_Toc497286194)

[4 Request for Change Requirements 8](#_Toc497286195)

[5 Planning for Change Management 10](#_Toc497286196)

[6 Create a Request for Change 12](#_Toc497286197)

[7 Submit a Request for Change 13](#_Toc497286198)

[8 Approve an RFC (TPR, SDM, CM) 15](#_Toc497286199)

[9 Communicate the Scheduled Maintenance 16](#_Toc497286200)

[10 Notify the Tactical Response Manager 18](#_Toc497286201)

[11 Execute an RFC 19](#_Toc497286202)

[12 Document the Completed Work 20](#_Toc497286203)

[13 Post the Change Validation 21](#_Toc497286204)

[14 Process Procedures for the Change Advisory Board 22](#_Toc497286205)

[15 Process Procedures for Emergency Changes 24](#_Toc497286206)

[16 Guidelines To Determine CR, SR or Break Fix 25](#_Toc497286207)

[17 Enforcement 26](#_Toc497286208)

[18 Roles and Responsibilities 27](#_Toc497286209)

[19 Metrics and Management Information 28](#_Toc497286210)

[19.1 Process Performance Measurable Metrics 28](#_Toc497286211)

[20 Responsibility 29](#_Toc497286212)

[**20.1** **Compliance Responsibility** 29](#_Toc497286213)

[**20.2** **Management Commitment** 29](#_Toc497286214)

[21 Exceptions 30](#_Toc497286215)

[22 Expiration 30](#_Toc497286216)

[23 Enforcement 30](#_Toc497286217)

[24 Appendices 31](#_Toc497286218)

[Appendix A - Change Management Process Flow 32](#_Toc497286219)

[Appendix B – Terms and Definitions 33](#_Toc497286220)

[Appendix C - References 37](#_Toc497286221)

[Appendix D - Distribution 38](#_Toc497286222)

List of Tables

[Table 1: Request for Change Toolsets 12](#_Toc497286223)

[Table 2: Planned RFC Minimum Lead Times 14](#_Toc497286224)

[Table 3: Guidelines to Determine CR, SR, and Break Fix 25](#_Toc497286225)

[Table 4: Roles and Responsibilities RACI 27](#_Toc497286226)

[Table 5: RACI Matrix Legend 27](#_Toc497286227)

[Table 6: Measure and Management Information 28](#_Toc497286228)

[Table A‑1: Change Management Process Flow 32](#_Toc497286229)

[Table B‑2: Terms and Definitions 33](#_Toc497286230)

[Table C‑3: References 37](#_Toc497286231)

[Table D‑4: Distribution Contacts 38](#_Toc497286232)

List of Figures

[Figure 4‑1: RFC Submittal Guidelines – Pre Change Requirements Template 9](#_Toc497286233)

# Process Overview

## Purpose

Change is necessary and inevitable for the needs of the business. The IBM Global Technology Services (GTS) Cloud Transformation Services (formerly Verizon), hereinafter referred to as “GCTS,” Change Management Process provides a controlled method to ensure that required changes are submitted, reviewed, approved, scheduled, and implemented with minimal disruptions to normal operations.

This document provides specific processes along with roles and responsibilities for carrying out planned and emergency Change Management actions.

This process documents the addendum policy statements supplemental to Supplemental to Information Technology Corporate Standard (ITCS) 104, Chapter 1, Section 1.6 Activity Auditing, Requirements 1, 2, and 3 and is developed to meet the control standards listed below addressing requirements specific to GCTS.

* ISO 2701:2013 - 14.2.3 and 14.2.4
* NIST 800-53 Rev 4 - CM-2(1)b, CM 3 b and d, IA-3, MA-2, SA-10b
* FedRAMP - CM-2(1)b, CM 3 b and d, IA-3, MA-2, SA-10b

## Scope

This process applies to all GCTS changes made within the:

* Internal Production Environment
* Managed Production Environments

These environments include all GCTS facilities supporting any asset(s) that exist in the environment. The process is necessary for meeting customer service-level requirements. This process governs all customer configuration items (CIs) that GCTS supports.

This process applies to ALL GCTS employees.

Exceptions to this process exist and are documented in the “Exclusions” section of [CHGM-00002 Change Management Policy](http://blueoperationsportal.apps.tmrk.corp/http:/mia20725sps496:46455/Quality%20Management/_layouts/DocIdRedir.aspx?ID=TP2DVDTPC4NT-125-74).

## Alignment with Corporate Policies

This document is a supplemental guideline that specifies certain requirements related to the GCTS. All documents considered for approval by the Governance of Risk, Compliance, and Quality (GRCQ) are sub-ordinate to, and supplements of, the Information Technology Corporate Standard (ITSC) 104, as well as the Business Conduct Guidelines, and World-Wide Records Management.

# Change Management Phases

GCTS implements our Change Management process in the following basic phases:

* **Planning for the Change**

This phase includes the following actions to ensure that all Requests for Change (RFCs) are successful:

* + Identifies that a change is needed
  + Determines the risk level of the change
  + Builds the change planning requirements
* **Managing the Change**

This phase reviews, approves, schedules, and communicates the change to all impacted parties.

* **Executing the Change**

This phase:

* + Requires an engineer to verify the work to be performed
  + Ensures that all required information and equipment are available
  + Implements the change
  + Validates that the change resulted in the expected outcome
  + Documents the work performed
  + Closes out the change

# Roles and Responsibilities

Many different people participate in the Change Management process. This section identifies the roles and responsibilities of GCTS employees who can request, review, approve, and execute an RFC.

## Requestor

The requestor initiates the change in the Change Management system. Typically, the requestor is the person or group that identifies the need for a change. This person or group can be from almost any internal team within GCTS. The requestor is usually a member of Client Services or one of the Service groups (for example, Support, Infrastructure, Implementation, Facilities.) In the Remote Application Management (RAM) environments the client can initiate RFCs. This role involves taking the following actions:

* Obtaining a supervisor’s or a manager’s approval for the change if required by the expected risk level
* Documenting and verifying that all RFC requirements have been met per the RFC requirements outlined in Section 4.
* Obtaining a Technical Peer Review (TPR) of the change prior to change submission. RAM changes follow a different process flow that requires Site Operation Center (SOC) Validations after RFC submission.

## Peer Reviewer

The peer reviewer evaluates the technical aspects of the change. This evaluation focuses on all aspects of the plan, ensuring that the proposed change is:

* Technically sound
* Capable of producing the desired outcome

The peer reviewer must be an engineer of equal or higher technical skillset than the requestor. This engineer can be from almost any technical team within GCTS, but is usually a member of one of the Service groups (for example, Support, Infrastructure, Implementation, Facilities.) This role involves taking the following actions:

* Ensuring that the CIs identified in the RFC match what is selected as impacted CIs in the change documentation
* Validating that the customer impact is accurate
* Verifying that the pre-change requirements are accurate and have been satisfied
* Validating all required step-by-step instructions for the change
* Ensuring that the listed duration for the change is accurate and includes time for rolling back the change, if required
* Verifying that the back-out steps and rollback plan are listed in the change and are valid
* Ensuring that the correct skill set is identified for the team/engineer performing the change
* Verifying that there are post-maintenance verification steps listed in the change and that they are correct to verify that the change has been implemented correctly
* Confirming that the change will accomplish the desired results to resolve the original issue
* Coordinating with all RFC stakeholders to clarify questions and provide feedback related to the approval or denial of the TPR

## Change Administrator

The Change Administrator (CA) reviews, approves/denies, schedules, and notifies all impacted parties of the RFC. Normal functional duties of the CA include, but are not limited to the following:

* Reviewing, filtering, classifying, and approving/denying all submitted RFCs
* Chairing periodic (that is, weekly) Change Advisory Board (CAB) review meetings
* Coordinating the RFC approval process
* Preventing potential conflicts by maintaining a Forward Scheduling of Change (FSoC)
* Ensuring that only authorized changes are approved and implemented, that changes are implemented in an acceptable timeframe in accordance with business requirements, and that changes are closed
* Generating regular and accurate Change Management reports
* Providing metrics for improving the Change Management process
* Coordinating timely communications to stakeholders and others who may be impacted prior to implementing a change

## Change Executor

This is the engineer or group within the organization that is assigned the responsibility of performing/executing the RFC. The Change Executor is the person who actually makes the configuration changes. This includes the following actions:

* Reading all RFC instructions and ensuring that they are clear and understood
* Escalate to the Tactical Response Manager (TRM) if any deviation is required
* Communicating the start of the maintenance to any persons identified as needing to know when the maintenance starts and completes
* This includes dialing into a conference bridge or directly calling a client based on service manager’s approval notes. Instructions can be found in pre change information.
* Executing the RFC as documented in the RFC and within the approved/scheduled maintenance window
* Providing post-maintenance communication to all identified parties after the maintenance has been completed
* Documenting all actions performed; including the identification of the engineer and delivery of all work minutes for work performed during the maintenance window
* Validating that the work had the desired results and the impacted CI is up and running as intended
* Closing the change as appropriate and identifying if the RFC was successful, was completed with issues, or failed

## Change Advisory Board

The GCTS CAB has representatives from all functional areas of the business. Each affected Director/Manager designates a representative. Each representative must be able to review, approve, and/or deny individual RFCs based on completeness, readiness, business impact, and business need.

## Executive Review Board

The GCTS Executive Review Board (ERB) has at least three executive management representatives from various parts of the business. At least one representative must be from Client Services and at least one must be from Service Delivery. The ERB reviews all RFCs classified as high risk (that is, Risk Levels 1 and 2). These proposed changes may have an impact on critical systems or infrastructure core. The requestor must get ERB approval prior to final CAB approval for Risk Level 1 or Risk Level 2 RFCs.

## CAB Executive Committee

The CAB Executive Committee (CAB/EC) must be available around the clock for emergency change request (ECR) approval. This group is typically referred to as the Emergency Change Advisory Board (ECAB) and members are listed in the following distribution list: GRP Emergency Change Notification. Emergency changes require approvals from the following five individuals:

* The manager of the person who requested the emergency RFC approval
* The director and the manager of the team that needs to execute the emergency RFC
* The on-call Change Administrator

If the ECR is for a CAB-level change or shared network changes outside the shared window, the following individuals must approve:

* The manager of the person who requested the emergency RFC approval
* The director and the manager of the team that needs to execute the emergency RFC
* The on-call Change Manager
* The VP of Service Delivery or said representative
* The VP/Director of Client Services or said representative

A separate process document governs ECRs.

## Tactical Response Manager

The Tactical Response Manager (TRM) is the on-shift manager responsible for engineering resources during his shift. The TRM is the escalation point for all incidents and ticketing related activities that surface during their shift. The change related activities include:

* Assign Incident Management Engineering (IME) resources for scheduled Change Request (CR)
* Contact assigned engineer for late started CR and resolve the issues
* Escalate client CR execution issues as requested by implementing engineer
* Approve RAM client changes on behalf of CA during off-hours by following the same Change Management (CM) policies and processes
* Manage change related escalations as reported by assigned engineer
* Ensuring environments are stable enough for change related maintenance activities
* Contacting Change Management on-call for any escalation requiring Change Management intervention

# Request for Change Requirements

RFCs are formalized descriptions of the change, the affected components, the business need, the expected risks and impacts, the required resources, and the approval status. RFCs must include the following:

* Unique identifier for the change
* List of impacted CIs that will be affected by the change
* Status of the change
* List of customers who will be affected by the change
* Clearly defined and documented scope of work
* Clearly defined impact statement
* Evidence of pre-submission fulfillment of all applicable RFC prerequisites
* Detailed implementation steps
* Results of peer review or SOC validation, with the exception of simple reboots
* Risk/severity level based on the Risk Impact Assessment Matrix; see Appendix B in CHGM-00002 Change Management Policy.
* Post-maintenance verification steps
* Rollback procedures
* Time estimates for implementation and rollback
* Confirmation from the data center (DC) verifying that equipment has been received at the appropriate DC, if applicable
* Pre-change Quality Assurance (QA) testing documented (for infrastructure RFCs only). (Testing can take place in a staging environment if lab testing is not an option.)
* Vendor ticket number and scope of work for vendor performed infrastructure events

The Requestor must submit all RFCs based on the RFC Submittal Guidelines.

All RFCs must follow Maintenance Window Guidelines.

These requirements shall be documented in the RFC. If the workflow is not built in, the requestor may use the following template shown in *Figure 4‑1: RFC Submittal Guidelines – Pre Change Requirements Template* .

E

|  |
| --- |
|  |
| Figure 4‑1: RFC Submittal Guidelines – Pre Change Requirements Template |

# Planning for Change Management

The planning process begins with the person who identified the need for the change. This is typically the person who raised/created the RFC. The planning process involves the following steps:

* Identifying requirements
* Verifying receipt of required hardware and software parts
* Identifying staffing resources
* Creating change documentation
* Coordinating the technical review of the RFC

The requestor must create the following change-planning documentation:

* Detailed implementation procedures
* Pre-change testing procedures
* Post-change validation steps
* Back-out procedures

The level of planning is usually directly proportional to the risk level of the change. The successful RFC has identified and ensured the following:

* Any impact to interrelated system(s) has been identified and considered
* The change conforms to all organizational standards for design, configuration, version, naming conventions, and management
* All participants understand the escalation paths
* The requestor has made “before” and “after” documentation available
* The requestor has planned and will implement document updates to all CIs

The RFC must also include the following:

* **Event Type**: (options are Emergency, Expedite, and Planned)
* **Risk Level (1-5)**: (1=High, 2=Medium, 3=Low, 4=Routine, 5=Standard) every change must have an associated risk and/or impact. Before an RFC can be submitted, the requestor must assess the risk and impact level of the change. Modeling the change in a lab environment or with a network-modeling tool can also help assess the risk of a proposed change. Based on the level of risk, the requestor must assign one of the risk categories as documented in the **Risk Impact Assessment Matrix;** reference **Appendix B in** CHGM-00002 Change Management Policy.
* **Security & Vulnerability assessments, if applicable**:
* **Date and Time Requested**:
* **Customer Affected**:
* **Equipment Location**:
* **Scope of Work/Purpose**: The purpose (or scope) of an RFC must include a complete technical definition and a description of the intent or purpose of the change. In addition, the RFC must include information describing what results are expected from the change and who will be impacted by the change. Those impacted may include business units, user groups, customers, servers and applications.
* **Team or engineer who will perform the work**:
* **Pre-Change Testing Conducted**: After the requestor has assessed the risk level, the infrastructure RFCs must undergo testing and validation. The risk level of the proposed change determines the level of testing and validation required. The requestor must fully document all test results and must include these results as an attachment to the RFC submission. Based on the risk-level, the requestor may use the Testing and Validation matrix to determine the required testing and validation.
* **TPR performed by**: All RFCs must undergo TPR prior to submission. The engineering review must focus on all aspects of the plan, ensuring that the proposed change is technically sound and capable of producing the desired outcome. The requestor must document the results of the TPR which will become a part of the RFC submission.
* **Detailed Implementation Steps**: All RFCs require detailed implementation steps. These are the step-by-step instructions of how to perform the change as well as any steps for how to document updates to CIs within the Configuration Management Database (CMDB.) The requestor may attach a document containing the standard operating procedure (SOP) if detailed information is not provided in this field. (Web links are not authorized as they can change.)
* **Quality Assurance Checklist of Steps/Post-Maintenance Verification**: If a document is attached, this field is not required as the information will be in the SOP.
* **Back-Out Process**: The requestor must list the back-out steps in the RFC in case the change needs to be rolled back. These steps must also include the point during implementation that everyone agrees to rollback to allow for complete rollback prior to the expiration of the maintenance window.
* **Maintenance Window Duration**: This must include the time to review the change requirements, the time to execute the change, and the time to roll back in the event a roll back is necessary.
* **Customer Impact**: The requestor must use this information to draft the customer notification for the requested maintenance.
* **Contact Information for the person requesting the change**: Typically, this includes the name, the cell phone number, and the email address.
* **Other Pertinent Information**: This can be any other piece of information that will be helpful to the engineer who will implement the change.

# Create a Request for Change

After the requestor has gathered all of the planning, testing, and related documentation, he can access the appropriate Change Management system and create/raise the RFC. Documents that explain how to create RFCs by toolset are posted on the GCTS Change Management SharePoint site at:  [http://bluedepartments.apps.tmrk.corp/ChangeManagement/default.aspx]( )

Currently, the requestor can use multiple systems to raise/create an RFC. If there is ever a question as to which system should be used to raise a change, the requestor must contact a Change Manager. Here are several RFC tools:

* Service Delivery Platform (SDP):
* [https://sdp.terremark.net/OSS.Login/Login.aspx]( https://sdp.terremark.net/OSS.Login/Login.aspx  ) 
  + For all Managed Hosting, IP Application Hosting (IPAH), GCTS RFCs
* Remedy- Remedy Modified version 6
  + For all RAM and Enterprise Cloud Managed Edition (ECME) RFCs

[The](#Table1) following table lists requests for change toolsets.

Table 1: Request for Change Toolsets

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | CR System | CR Calendar | Notification | CAB |
| RAM (Clients) | Remedy\* | TotalView\*\* | Remedy | N/A |
| Enterprise Cloud Managed Edition (Clients) | Remedy | TotalView | Remedy | N/A |
| IPAH (Clients) | SDP | SDP | SDP | N/A |
| RAM (Infrastructure) | Remedy | TotalView | Outlook®, Remedy | Remedy |
| ECME, Global Inbound Services (GIS) (Infrastructure) | Remedy | TotalView | Outage Notification | Remedy |
| IPAH (Infrastructure) | SDP | SDP | SDP | SDP |
| GCTS | SDP | SDP | SDP | SDP |

*\* Remedy -Ticketing system currently in use by RAM/ECME customers and some data center locations.*

*\*\* TotalView© – Demonstrate Remote Application Management Services Portal.*

# Submit a Request for Change

For a planned change, there may be a delay between the RFC submission and the approval/scheduling of an RFC. This delay provides CAs time to ensure the:

* Requestor has included all required RFC information
* Requestor has given adequate advance notice to those individuals who will be affected by the change, allowing for sufficient time to prepare for the change event

Requestors who submit RFCs outside of the posted timelines below may be denied, may be rescheduled, or may require Emergency Change Request (ECR) submission.

* A requestor can submit an ECR for CAB/EC approval at any time

**Note**: The requestor can use an ECR only when a situation arises that is unplanned but critical in nature. The requestor must NOT use an ECR as a substitute for poor planning. He or she must always follow up the submission of an ECR with a telephone call to the CA on call and an email. He or she must make the phone call to **469-461-9348**. If the ECR is not raised in the SDP, the requestor must send an email to the Distribution List: [GRP Emergency Change Notification](mailto:emergencychangenotification@terremark.com) requesting approval.

* A requestor can submit an expedited RFC for approval at any time. Examples of expedited RFCs include:
  + Dedicated Customer Environment (DCE) changes for dedicated customer network gear. RAM changes that have specific customer timelines required by Service Level Agreements (SLAs)
* The requestor must submit a planned RFC with the minimum lead times as outlined in [Table 2](#Table2).
* All RFCs that are presented in the CAB must have:
  + An Impact Assessment (IA) Score Sheet
  + A Pre-change Testing/QA form
  + A clearly define customer impact statement in addition to all other RFC requirements.
* The requestor must submit all CAB-level RFCs prior to the next CAB meeting. This will allow for documentation of the RFC on the CAB agenda. See submission cutoff times below:
  + **CAB Steering Committee**: Prior to 10:00 (ET) on Monday for that Tuesday’s weekly meeting, the requestor must submit through the appropriate Change Management toolset all changes that require review during the weekly CAB steering committee meeting. The requestor must consider advance notification requirements during planning sessions to ensure adequate notification timelines after CAB Steering Committee approval of the change.
  + **CAB**: Prior to 18:00 (ET) on Monday for that Wednesday’s weekly meeting, the requestor must submit through the appropriate Change Management toolset all changes that require review during the weekly CAB meeting. The requestor must consider advance notification requirements during planning session to ensure adequate notification timelines after CAB approval of the change.

Table 2: Planned RFC Minimum Lead Times

| Risk Level | Minimum Lead Time for RFC submission |
| --- | --- |
| 1 | Must be presented in CAB four weeks in advance of requested execution date. |
| 2 | Must be presented in CAB two weeks in advance of requested execution date. |
| 3 | Must be presented in CAB one week in advance of requested execution date. |
| **4** | **Server changes**: If submitted by 16:00 (ET) can be scheduled for the next shift (20:00 ET) on the same day. (Refer to CHGM-00002 Appendix E, Table E-1: Maintenance Window Guidelines.)  **Shared network**: If submitted by 16:00 (ET,) can be scheduled in the next shared network window. (Refer to CHGM-00002 Appendix E, Table E-1: Maintenance Window Guidelines.)  **Dedicated customer environments**: If emergency in nature, can be scheduled as soon as the process allows for required change documentation.  Change submission cutoffs by toolset for changes that meet normal scheduling criteria:   * **SDP**: RFCs must be submitted prior to 16:00 ET for the next shift. Weekend cut-off time is 16:00 ET on Friday. * **REMEDY**: RFC submissions per customer SLA do not require an ECR; CAB-level infrastructure RFCs must be submitted to allow for the normal CAB review process.  |  | | --- | | Weekend work is considered work between 17:00 ET on Friday through 08:00 ET on Monday. | |

**Note**: The CAB reserves the right to have the Requestor reschedule changes (regardless of Risk Level) if the change is determined to be conflicting or introducing unacceptable risk to any other RFC scheduled within the same change review period.

For a planned change a sufficient delay between RFC approval and execution is necessary to ensure a notice communication for those being impacted. Allow sufficient time to prepare for this Change Event.

# Approve an RFC (TPR, SDM, CM)

The RFC approval process is standard no matter which tool is used to raise the RFC. After the requestor has created an RFC, he must route the RFC for a Technical Peer Review (TPR). Upon completion of the TPR, the peer reviewer must route the RFC for CA review, approval, and scheduling. Service Deliver Manager (SDM) approval/client advocate may be required prior to CA scheduling a change. If an RFC is incomplete or not ready for scheduling, the CA must notify the requestor that the RFC cannot be scheduled in the existing state. This notification must include specifics as to what is missing or incorrect with the submitted RFC.

# Communicate the Scheduled Maintenance

Once the RFC has been approved and scheduled on the FSoC, the requestor must next communicate the details of the scheduled maintenance activity to the end client(s) and all essential internal teams. Communication is essential to:

* Set expectations
* Convey scheduled downtimes
* Align adequate support resources

For RFCs that may have customer impacts, the requestor must send notifications well in advance of the scheduled implementation date.

* All GCTS-mandated infrastructure RFCs shall adhere to the following advanced notification guidelines if notification is required by CAB or Client Services:
  + **No customer impact**: 7 days advanced notification
  + **Expected customer impact**: 14 days advanced notification

The requestor must identify who may be impacted by a change prior to RFC submission and must inform Change Management. Notifications must include those to customers and vendors as well as those to internal GCTS departments or global offices that may be affected. The requestor may need to use separate internal and external communications to properly convey this notification to the change management team. The requestor must send notifications to CA by email and the notifications must be clear and concise, and must be written in a manner that can easily be understood by non-technical personnel.

The requestor can use the following notification template attached ***rt found.***

**

# Notify the Tactical Response Manager

Prior to the start of a planned infrastructure RFC for all changes of Risk Levels 1 through 3, the requestor must notify the [GSS.Global.All@one.verizon.com](mailto:GSS.Global.All@one.verizon.com). Based on the overall operational status at that time, the TRM must determine if the RFC should be implemented as planned or postponed until more favorable condition exists.

If approved, the engineer or team assigned to the RFC can implement the RFC as planned. Immediately upon completion of the RFC, whether successful or not, the engineer must notify the GSS.Global.All@one.verizon.com. If the TRM denies implementation of the RFC, the Requestor must provide a new date and/or time and must resubmit the RFC for CAB review and approval.

For coordinating communications between team members carrying out large or very intricate changes, the requestor should consider using a telephone conference bridge as part of the change planning process.

Communication path during change:

* Schedule change or extension 🡪 TRM, Service Manager, Contacts listed in CR
* Encounter Technical Problem 🡪 TRM, Service Manager, Contacts listed in CR
* Change Process Questions 🡪 Change Management On-call
* Caused Outage 🡪 TRM, Service Manager, Failed Change DL address GRP.Failed.Change.Submit@one.verizon.com

# Execute an RFC

* Do not begin work on changes that have not completed the approval process. Only "Scheduled" changes that are "Ready to Start" or “Approved & Scheduled” on FSOC can be executed.
* The implementation engineers are responsible for monitoring the scheduled CRs on the change calendar.
* Review the change for all work related steps; escalate to TRM if there is any confusion
* Communicating the start of the maintenance to any persons identified as needing to know when the maintenance starts and completes
* This includes dialing into a conference bridge or directly calling a client based on service manager’s approval notes. Instructions can be found in pre change information.
* Start and Complete the CR within the maintenance window. Escalate to the on-shift TRM when changes starting over 15 minutes late or changes exceeding scheduled completion time by over 15 minutes. If a client change will not be completed by the Scheduled End Time, the engineer must call the SDM or submitter to request an extension.
* Changes that will send alerts to the alert board must be announced to the Global Support Services Customer Service Representative (GSS CSR) or TRM when starting and completing a CR.
* GSS Engineers working on a change are responsible for owning the alerts they generate during the change and for one hour after the change has been completed.
* Update the Work Log often (and save).
* Document your activities. It is not sufficient to say that you completed the change as requested. Include significant steps, comments and output to demonstrate what was done. When applicable, entries that display hostname, username and directory listings are extremely helpful when reviewing changes later. If command output gets too long, copy it into a file, attach the file to the Change Request and reference the attachment in the Work Log.
* If the request includes a note or instruction to be extra special careful to do a specific step, include a confirmation comment in the Work Log when you actually perform that step.

# Document the Completed Work

The engineer or group within the organization that is responsible to perform/execute the RFC must document the work performed during the implementation of an RFC. This includes but is not limited to the following:

* Documenting all actions performed
* Include their name as the engineer
* Documenting all work minutes performed during the maintenance window
* Documenting verification steps to ensure the outcome of the RFC

# Post the Change Validation

All changes must include post-change validation. This is typically in the form of QA steps to test and evaluate the outcome of an RFC. The requestor must include validation steps to ensure that the desired outcome of the RFC has been met. This includes ensuring that no security or vulnerability risks have been introduced into the secured environment. If the RFC did not meet the desired outcome, then the Change Executor must follow the back-out process or fail the change and resubmit the change when all issues have been addressed.

Reference [*Appendix A: Change Management Process Flow*](#AppendixA)

# Process Procedures for the Change Advisory Board

GCTS requires weekly CAB meetings in accordance with Change Management Policies. The requestor must ensure that all changes that meet the CAB criteria are managed in a standardized manner to ensure that the change receives the proper review and approval prior to implementation. The requestor must assign an RFC risk level based on the expected impact. GCTS Change Management reviews all RFCs for risk level and surfaces every change with a risk level of 1, 2, or 3 to the CAB for review.

When presenting an RFC to the CAB Committee, the requestor must be prepared to explain/discuss the following:

* Reason for the change
* Planning and testing conducted
* Risk level
* Potential impact to the customer or to the business
* Detailed implementation steps
* Post-maintenance verification and testing
* Roll-back procedures

The GCTS CAB is governed by the CAB Policy and must adhere to the guidelines below:

* The CAB will meet weekly to review any RFCs that have been submitted that have the potential to impact Infrastructure or multiple customers.
* The Change Management team must compile and disseminate the weekly CAB agendas and must provide oversight of the weekly CAB meetings.
* On the day before each CAB meeting, the Change Management team must publish and release to the CAB the agenda. The CAB may deny any RFC that is:
  + Incomplete
  + Without merit or justification
  + Poses too great a risk in its present form
* The CAB can refer to the ERB for review and consideration any RFC that the CAB considers High Risk. Change Management Team members can also refer any RFC for ERB review if the CAB cannot reach a unanimous decision.
* All RFCs that are presented in the CAB must have:
  + An Risk Assessment Score Sheet
  + A Pre-change Testing/QA form
  + A clearly defined impact statement
  + All other RFC requirements
* The requestor must submit all CAB-level RFCs prior to the next CAB meeting. This will allow for documentation of the RFC on the CAB agenda. Reference Submission cutoff times in Section [7](#SUbmitCR).

For more specifics regarding the GCTS CAB, refer to the GCTS CAB Process Overview.

# Process Procedures for Emergency Changes

GCTS has an emergency change procedure in place to detail the steps necessary to request approval for an ECR. Any change with a Risk/Impact level 1-4 that must be completed before the normal process must adhere to the ECR procedure. This also includes any:

* RFC submitted during a weekend or during a holiday that needs to be implemented during that time period
* RFCs submitted during a shift that need to be performed during that same shift

All ECRs require at a minimum approvals from the:

* The Manager of the Requestor
* The Director of the Group performing the change
* A member of the Change Management team

For more specifics regarding emergency changes, refer to the GCTS ECR procedure.

# Guidelines To Determine CR, SR or Break Fix

Table 3: Guidelines to Determine CR, SR, and Break Fix

| CR (Change Request) | SR (Service request/TICKET) | Break Fix |
| --- | --- | --- |
| Change as it pertains to GCTS Change Management is defined as any modification to fit, form, or function of a GCTS system or a system managed by GCTS.  **Note**: This includes any changes to production devices as well as introducing any devices into production. | A Service Request is a request from a user for advice, information or access to some IT service. | An Incident ticket that requires an immediate remediation to restore the loss of a service. The Break Fix on GCTS shared environment must require management level approval. |
| **Examples**:   * Hardware * Software * Configuration of computers * Networks * Databases * Communications equipment * Any other component introduced into the GCTS environment that may impact a customer Service Level Agreement (SLA) either directly or indirectly. | **Examples**:   * User asking for a password reset * Customer request for a report * Customer asking for details from a previous Problem or Change * Customer asking if specific network port status or parameters of a configuration file * Customer is requesting additional/new services not previously purchased * Contact information for notification or escalation needs to be changed | **Examples**:   * System outage * Network outage * Security vulnerability under attack |
| **Require**: Request For Change (RFC) | **Require**: Service Request (SR)  **Note**: All change management policy criteria must be followed. (If making a change in a production environment, a CR must be raised) | **Require**: Incident ticket or Problem ticket |
| Approval:   * Change Process section 8 * Change Policy section 2.3 | **Approval**:   * Engineer review for confirmation of SR category | **Approval**:   * GCTS management Level |

# Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Roles and Responsibilities

Table 4: Roles and Responsibilities RACI

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Process Name | Requestor | Peer Viewer | SDM /  Manager | Change Admin | Change Executor | CAB /  ECAB | TRM |
| 5. Planning | AR | C | C | C | C |  |  |
| 6. Creating | AR | C | C | C | C |  |  |
| 7. Submitting | R | AR | C | C | I |  |  |
| 8. Approving | I | A | R | R | C | R | I |
| 9. Communicating | I |  | C | AR | I | I | I |
| 10. Notifying TRM | I | I | I | I | AR |  | C |
| 11. Executing | I |  | I | I | AR |  | C |
| 12. Documenting |  |  |  | I | AR |  | C |
| 13. Validating |  |  |  | I | AR |  | C |
| 14. CAB | R |  | I | C | C | A | I |
| 15. ECR | R | C | I | C | C | A | I |

Table 5: RACI Matrix Legend

| RACI | TERM | DEFINITION |
| --- | --- | --- |
| R | Responsible | The person who does the work to complete the task. They are responsible for getting the work done. |
| A | Accountable | The person who is accountable for the correct and thorough completion of the task. |
| C | Consulted | The people who provide information for the project and with whom there is a two-way communication. This is usually several people, often subject matter experts. |
| I | Informed | The people who are kept informed about progress and with whom there is a one-way communication. These people are affected by the outcome of the tasks and need to be kept up-to-date. |
| AR | Accountable and Responsible | The person who does the work to complete the task and are accountable for the correct and thorough completion of the task. |

# Metrics and Management Information

## Process Performance Measurable Metrics

The following is a summary of the metrics that should be collected to provide performance information for management review on a regular basis.

Table 6: Measure and Management Information

|  |  |  |
| --- | --- | --- |
| Metric | Description and Value | Key Performance Indicator (KPI) |
| Volume of Change Requests (CRs) | The number of Change Request both Manual and Automated tracked on monthly basis. | Success Rate of Manual and Automated CRs > 98% |
| Volume of Emergency CRs | The number of Emergency CRs requested monthly  (Less than 1% of the total change volume) | Success Rate of Emergency CRs > 98% |
| Volume of Infrastructure (CAB Level) CRs | The number of Infrastructure changes requested monthly | Success Rate of Infrastructure (CAB Level) CRs > 98% |
| Outage Related to Failed (CAB Level) CRs | The number of CRs that “failed” and caused outage per month | Failed CRs identified Root Cause Analysis (RCA) & Permanent Corrective Action (PCA) |
| Identified Unauthorized CRs | The number of CRs executed without authorization | Identified and preventative action in place |

1. **Responsibility**

The GTCS Business Owner (BO) or Information Resource Custodian (IRC) of record is responsible and held accountable for enforcement of published policy, process, and procedure documentation.

It is the responsibility of all personnel to know, understand, and conform to the policies set in the ITSC 104, Business Conduct Guidelines, World-Wide Records Management, and others as they apply to all GCTS employees.

* 1. **Compliance Responsibility**

Compliance with security standards and practices addressed in this document are subject to applicable law. Conflicts with local legislation or regulation shall be brought to the attention of GRCQ Council and coordinated with the responsible security executive for resolution.

*Important: Nothing in this document should be taken as justification to circumvent existing IBM Corporate policies, standards, or management direction.*

* 1. **Management Commitment**

GCTS has established the GRCQ to serve as a forum for all stakeholders with responsibility for maintaining the security of the GCTS information technology environment, both internal and customer serving.

This policy has been managed by SECM-00089 Policy Management Process and approved by the GRCQ Council.

1. **Exceptions**

Exceptions to this process must be approved by the GCTS BO or IRC of record as defined by the governing/serving Lightweight Enterprise Governance Organization (LEGO), as defined by LEGO Program Charter and the LEGO Knowledge Management Charter.

1. **Expiration**

Unless readopted, this document expires three (3) years from the date of approval.

1. **Enforcement**

Any employee found to have violated this process may be subject to disciplinary action, up to and including termination of employment.

# Appendices

Appendix A - Change Management Process Flow 32

Appendix B – Terms and Definitions 33

Appendix C - References 37

Appendix D - Distribution 38

Appendix - Change Management Process Flow

Table A‑1: Change Management Process Flow



Appendix B – Terms and Definitions

Table B‑2: Terms and Definitions

|  |  |
| --- | --- |
| BO | Business Owner |
| Break Fix | An Incident ticket that required an immediate remediation to restore a loss of service. The Break Fix on GCTS shared environment must require management level approval. |
| CA | Change Administrator |
| Change | Change as it pertains to GCTS Change Management is defined as any modification to fit, form, or function of a GCTS system or a system managed by GCTS. These systems include:   * Hardware * Software * Configuration of computers * Networks * Databases * Communications equipment * Any other component introduced into the GCTS environment that may impact a customer Service Level Agreement (SLA) either directly or indirectly.   **Note:** This includes any changes to production devices as well as introducing any devices into production. |
| Change Advisory Board (CAB) | The GCTS CAB will consist of representatives from various functional groups within the Business who are authorized and capable of reviewing, approving and/or denying individual RFCs based on:   * Completeness * Readiness * Business impact * Business need |
| Change Management Administrator (CMA) | An individual within the organization who acts as a coordinator for change process details. |
| CI | Configuration Items |
| Client Advocate | Refers to the different ways clients are represented in GCTS . Some clients have Service Managers and some have Client Executives. This is the customer-facing employee who owns the client relationship and can authorize changes on the client’s behalf. |
| CM | Change Management |
| CMDB | Configuration Management Database |
| CR | Change Request |
| CSR | Customer Service Request |
| DC | Data Center |
| DCE | Dedicated Customer Environment |
| ECAB | Emergency Change Advisory Board |
| ECME | Enterprise Cloud Managed Edition |
| Emergency Change Request (ECR) | An RFC that needs to happen outside of standard maintenance window guidelines. |
| ET | Eastern Time |
| Executive Review Board (ERB) | The GCTS ERB will consist of at least three Executive Management representatives within the company. The ERB must review and approve any RFC that:   * Is high risk * Will have high impact to critical systems or infrastructure   ERB review and approval is required before the CAB can provide final approval. |
| Forward Schedule of Change (FSoC) | The calendar view of approved changes maintained and communicated to relevant parties to avoid event collisions. |
| GCTS | Global Technology Services (GTS) Cloud Transformation Services (formerly Verizon) |
| GRCQ | Governance of Risk, Compliance, and Quality |
| GSS | Global Support Services |
| GTS | Global Technology Services |
| IME | Incident Management Engineering |
| IPAH | IP Application Hosting |
| IRC | Information Resource Custodian |
| IRC | Information resource Custodian |
| ITCS | Information Technology Corporate Standards |
| LEGO | Lightweight Enterprise Governance Organization |
| Notification for Change (NFC) | Any change performed by client or vendor - that the Service Manager raises on behalf of a vendor or customer that is performing maintenance on their environments. GCTS should receive advance notification to allow for customer notification and change documentation on the FSoC. |
| QA | Quality Assurance |
| RAM | Remote Application Management |
| Request for Change (RFC) | The formal descriptions of the change are raised within the Change Management tool. The RFC will include:   * Components affected * Business need * Detailed implementation steps * Risk and impact assessment * Resource requirements * Technical peer review (TPR) * Approval status |
| SDM | Service Deliver Manager |
| SDP | Service Delivery Platform |
| Service Request (SR) | A Service Request is a request from a user for advice, information or access to some IT service. Some examples:   * User asking for a password reset * Customer request for a report * Customer asking for details from a previous Problem or Change * Customer asking if specific network port status or parameters of a configuration file * Customer is requesting additional/new services not previously purchased   Contact information for notification or escalation needs to be changed |
| Site Operation Center (SOC) Validation | A form of technical review of a proposed change. A designated SOC engineer performs this review. The engineering review will focus on all aspects of the plan, ensuring the proposed change is:   * Technically sound * Capable of producing the desired outcome   A technical peer of the engineer that created the RFC will document the results of the SOC validation, which become a part of the RFC submission. A SOC Validation is typically associated with:   * RAM * ECME (Enterprise Cloud Managed Edition) changes |
| SLAs | Service Level Agreements |
| SOP | Standard Operating Procedure |
| Standard Change | CAB Pre-approved requests for Standard Change events that are low risk, standardized where the risk and impact is documented, known, clearly understood and predictable. Standard Change will be authorized without a Change Request. Approved Standard Changes can be raised in the ticketing module according to approval parameters and restrictions documented in the Standard Change approval document. |
| TCC | Technical Coordination Committee |
| Technical Peer Review (TPR) | The engineering review will focus on all aspects of the plan, ensuring the proposed change is:   * Technically sound * Capable of producing the desired outcome   A technical peer of the engineer that created the RFC will document the results of the TPR, which become a part of the RFC submission. |
| Total View Change Calendar (TVCC) | The calendar view of RAM and ECME changes maintained and communicated to relevant parties to manage and monitor change events. This is the:   * FSoC for RAM & ECME |
| TRM | Tactical Response Manager |
| Unauthorized Change | A change made to the GCTS or customer’s IT infrastructure that violated defined and agreed upon Change policies. |

Appendix C - References

Table C‑3: References

| Document Number | Document Title |
| --- | --- |
| CHGM-00003 | [CHGM-00003 TQM Facilities Operations Change Management Process Overview](http://blueoperationsportal.apps.tmrk.corp/Quality%20Management/Public%20Documents/Service%20Delivery/Change%20Mgmt/CHGM-00003%20TQM%20Facilities%20Operations%20Change%20Management%20Process%20Overview.pdf) |
| CIO 122 | IBM Worldwide Records Management |
| IBM BCG | IBM Business Conduct Guidelines |
| ITCS 104 | IBM Information Technology Corporate Standard 104 |
| SECM-00089 | [SECM-00089 Policy Management Process](http://blueoperationsportal.apps.tmrk.corp/Quality%20Management/Public%20Documents/Security%20Management/SECM-00089%20Policy%20Management%20Process.pdf) |

Appendix D - Distribution

Table D‑4: Distribution Contacts

| Name/Role | Contact Information |
| --- | --- |
| Document Management | [Document.Management@verizon.com](mailto:Document.Management@verizon.com); Document\_Management@wwpdl.vnet.ibm.com |
| GCTS GRCQ Council | [GCTS\_GRCQ\_Council@wwpdl.vnet.ibm.com](mailto:GCTS_GRCQ_Council@wwpdl.vnet.ibm.com) |
| GCTS TCC | [GCTS\_TCC@wwpdl.vnet.ibm.com](mailto:GCTS_TCC@wwpdl.vnet.ibm.com) |
| Global Support | [GSS.Global.All@one.verizon.com](mailto:GSS.Global.All@one.verizon.com) |
| Global Operations Change Management | [grpglobalchangemanagement@verizon.com](mailto:grpglobalchangemanagement@verizon.com) |
| Shannon Soland |  |