Change Management

change management POLICY

Verizon Enterprise Solutions Cloud and Data Center Services Supplemental to Verizon CPI-810 5.0 Operations Management Section 05.1.07 Operational Change Control

© 2013, 2014, 2015, 2016, 2017 Verizon. All Rights Reserved.

The Verizon name and logo and all other names, logos, and slogans identifying Verizon’s products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

Revision History

| version | Date | APPROVED BY | Description of the Change |
| --- | --- | --- | --- |
| 0.1 | 27-Jan-2010 | Kay Lipps | Initial Draft |
| 0.2 | 26-Apr-2010 | Kay Lipps | Combined Change. |
| 0.3 | 01-Oct-2010 | Kay Lipps | Updated Maintenance Window Guidelines and policy Exclusions. |
| 0.4 | 16-Mar-2011 | Kay Lipps | Added requirements for Post Maintenance Validation. |
| 0.9 | 24-May-2013 | Kay Lipps | Integrate existing Terremark Change with newly added Services.  Change Section 3.9.1 title. Table C-1, Risk Level 4: added Stem “Change submission cut-offs” and following bullet list. |
| 1.0 | 03-Jun-2013 | Kay Lipps | Initial release |
| 1.1 | 27-Jul-2013 | Marc Verstraeten | QA check – fix file number in header |
| 2.0 | 19-Jun-2014 | Kay Lipps | Policy renewal and template format updated. |
| 2.1 | 21-Aug-2014 | Kay Lipps | Update submission Guidelines in Table C-1 |
| 2.2 | 23-Sep-2014 | Kay Lipps | QA update with new DMS template |
| 3.0 | 28-Oct-2015 | Kay Lipps | Annual review and updates, added Standard Change to 2.9.3 and Appendix B. |
| 3.1 | 03-Nov-2015 |  | Senior Analyst (Penny Poe) Review and edits:   * Analysed against CPI-810 05.1.07 Operations Change Control, 800-53 CM-3 Configuration Change Control, PCI DSS 6.4 and 6.4.5, HIPPA Standards * Inserted hyperlinks for reference docs |
| 3.2 | 06-Nov-2015 |  | Addressed GSS comments – TCC Review 11.9.2015 |
| 4.0 | 10-Nov-2015 | TCC Approved | Suggested changes to Section 2.9.4/TCC Approved |
| 4.1 |  |  | Updated Vendor events in section 2.1 & Appendix A (Service Request, Unauthorized Change) |
| 4.2 | 29-Feb-2016 | Penny Poe | Policy Management Review and Approval for TCC Review – Document will only require TCC Approval for Republishing since the changes were minor and did not change the overall context of the Policy |
| 4.3 | 14-Mar-2016 | TCC Approved | Approved for republishing |
| 4.4 | 07-Mar-2017 |  | Checkout for annual review, minor template updates |
| 5.0 | 12-Apr-2017 | Kay Lipps | Approved for republishing |

Table of Contents

[1 Overview 1](#_Toc479834791)

[1.1 Purpose 1](#_Toc479834792)

[1.2 Scope 1](#_Toc479834793)

[1.2.1 Personnel Covered 1](#_Toc479834794)

[1.2.2 Alignment with Verizon CPS-810, CPI-810, and other Corporate Policies 1](#_Toc479834795)

[1.2.3 Environments Covered 1](#_Toc479834796)

[2 Policy 2](#_Toc479834797)

[2.1 Requests for Change Policies 2](#_Toc479834798)

[2.2 Prioritization Policies 2](#_Toc479834799)

[2.3 Change Approval Policies 3](#_Toc479834800)

[2.4 Change Scheduling Policies 3](#_Toc479834801)

[2.5 Release and Notification Policies 3](#_Toc479834802)

[2.6 Testing and Rollback Policies 4](#_Toc479834803)

[2.7 Change Implementation Policies 4](#_Toc479834804)

[2.8 Post-Change Documentation and Reporting Policies 4](#_Toc479834805)

[2.9 Policy Exclusions 5](#_Toc479834806)

[2.9.1 Hosting Dedicated Network Gear (Dedicated Customer Environment) 5](#_Toc479834807)

[2.9.2 Remote Application Management 5](#_Toc479834808)

[2.9.3 Standard Changes 5](#_Toc479834809)

[2.9.4 Contractually-Excluded Products 5](#_Toc479834810)

[3 Responsibility 6](#_Toc479834811)

[3.1 Compliance Responsibility 6](#_Toc479834812)

[3.2 Management Commitment 6](#_Toc479834813)

[4 Exceptions 7](#_Toc479834814)

[5 Expiration 7](#_Toc479834815)

[6 Enforcement 7](#_Toc479834816)

[7 Appendices 8](#_Toc479834817)

[Appendix A - Terms and Definitions 9](#_Toc479834818)

[Appendix B - Risk and Impact Assessment 12](#_Toc479834819)

[Appendix C - RFC Submission Guidelines 13](#_Toc479834820)

[Appendix D - OCRB and MASTARS Submission Guidelines 14](#_Toc479834821)

[Appendix E - Maintenance Window Guidelines 15](#_Toc479834822)

[Appendix F - References 16](#_Toc479834823)

[Appendix G - Distribution 17](#_Toc479834824)

List of TABLES

[Table A‑1: Terms and Definitions 9](#_Toc479834825)

[Table B-1: Risk and Impact Assessment 12](#_Toc479834826)

[Table C-1: RFC Submission Guidelines 13](#_Toc479834827)

[Table E-1: Maintenance Windows Guidelines 15](#_Toc479834828)

[Table F‑1: References 16](#_Toc479834829)

[Table G‑1: Distribution Contacts 17](#_Toc479834830)

List of Figures

**No table of figures entries found.**

# Overview

## Purpose

The purpose of the Verizon Enterprise Solutions (VES) Cloud and Data Center Services, hereinafter referred to as “Cloud,” Change Management Policy establishes a controlled process to ensure that all changes are submitted, reviewed, approved, scheduled, and implemented with minimal impact to service quality. The following policies shall govern the performance of Change Management activities in order to ensure the sustainable development, implementation, and improvement of services.

## Scope

### Personnel Covered

This policy applies to all changes made within the Cloud internal production environment and Cloud managed production environments. This includes all customer Configuration Items (CIs) that Cloud is responsible to support.

See *Section 2.9* for exceptions to this policy.

### Alignment with Verizon CPS-810, CPI-810, and other Corporate Policies

This document is a supplemental policy that specifies certain requirements related to Cloud. All policies considered for approval by the Cloud Information Security Council (CICS) are sub-ordinate to, and supplements of, Verizon Corporate Policy CPS-810 and Corporate Policy Instruction CPI-810, as well as other relevant Verizon policies, such as the Code of Conduct, Verizon CPS-303, and Verizon CPS-130.

### Environments Covered

Unless otherwise noted, the controls outlined within this policy apply to all equipment that Cloud owns, manages, or leases.

# Policy

## Request for Change (RFC) Policies

* All RFC shall be recorded.
* Planned RFCs shall have a clearly-defined and documented scope.
* A procedure with RFC requirements shall be documented and enforced for RFC submittals.
* All RFCs shall include Detailed Implementation Steps.
* All Detailed Implementation Steps shall receive a Peer Review or Site Operation Center (SOC) Validation with the exception of simple reboots.
* All RFCs shall include an associated Risk/Severity Level. Reference Appendix B, Table B-1.
* All RFCs shall have a clearly defined impact statement.
* All RFCs shall be submitted based on the RFC Submittal Guidelines. Reference Appendix C, Table C-1.
* All RFCs shall follow Maintenance Window Guidelines. Reference Appendix E, Table E-1.
* All RFCs shall include Post Maintenance Verification Steps.
* All RFCs shall include rollback procedures.
* All RFCs shall include time estimates for roll forward and rollback.
* All hardware-related RFCs shall include confirmation from the Data Center (DC) verifying that the DC has received all equipment at the appropriate DC.
* All applicable prerequisites to the RFC shall be fulfilled prior to submittal.
* All Infrastructure RFCs shall have Pre-Change activities documented to include quality assurance testing with validated results. Testing can take place in a staging/live environment if lab testing is not an option.
* All vendor-performed infrastructure maintenance events shall include a vendor ticket number and scope of work. Peer Review is not required for vendor performed work.

All RFCs that require DC smart / remote hands to execute work will require a ticket from the DC confirming availability of the personnel to perform the work.

## Prioritization Policies

* All RFCs shall be assessed for their risk, impact, and business benefit based on the Risk Level Matrix. Reference Appendix B, Table B-1.
* All RFCs, excluding patches that are not prioritized as an Emergency Change Request (ECR) shall be considered to have a priority of ‘normal.’
* Emergency RFCs shall go through an Emergency Request for Change Procedure requiring additional levels of approval and denoting the priority of these changes as Emergency changes.
* Facility changes shall be governed using [CHGM-00003 Facilities Operations Change Management Process Guide](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Service%20Delivery/Change%20Mgmt/CHGM-00003%20TQM%20Facilities%20Operations%20Change%20Management%20Process%20Overview_old%20template.pdf).

## Change Approval Policies

* All RFCs shall have Client or Client Advocate review.
* All Service Delivery Manager (SDM) approval containing contact information shall clearly spell out phone number or conference details.
* All RFCs shall have Change Administrator review and all other appropriate approvals.
* There shall be policies and procedures to control the approval of ECRs
* There shall be a Change Process Overview to govern the requirements of a Change Advisory Board (CAB) meeting.
* The CAB must approve all RFCs with Risk Levels 1, 2, and 3. Reference Appendix B, Table B-1.
* The CAB can escalate any RFC with Risk Level 2 and 3 to the Executive Review Board (ERB) at any time.
* The CAB will review competing changes to determine priority.
* There shall be a change procedure to govern CAB Pre Approved changes
* There shall be a change procedure to govern CAB Approved Standard changes

## Change Scheduling Policies

* All approved RFCs shall be scheduled on a Forward Schedule of Change (FSoC), either in the change management module of the Service Delivery Platform (SDP) or on the Total View Change Calendar (TVCC).
* All approved RFCs shall be scheduled based on the approved implementation date.

## Release and Notification Policies

* All approved and scheduled RFCs shall include advanced notification to appropriate parties.
* All Verizon mandated infrastructure RFCs shall adhere to the following advanced notification guidelines:
  + No customer impact – 7 days’ advanced notification (Note)
  + Expected customer impact – 14 days’ advanced notification (Note)

**Note:** The only exception to the advanced notification guidelines are RFCs approved using the ECR Procedure.

## Testing and Rollback Policies

* All Infrastructure RFCs shall have Pre-Change activities documented to include Quality Assurance (QA) testing with validated results. Testing can take place in a staging/live environment if lab testing is not an option.
* All RFCs shall include rollback procedures that describe the manner in which the change shall be reversed or remedied if unsuccessful or in the event testing is not feasible.
* The scheduled maintenance window should include the time estimates required to roll back the change. The roll back plan should state specifically at what point during the change roll back should take place, if roll back is required. For example, if the change takes 30 minutes and the roll back plan takes 10 minutes; then the maintenance window should be scheduled for 40 minutes.

## Change Implementation Policies

* All RFCs shall be implemented in a controlled manner. The assigned engineer shall:
  + Review all RFC information prior to executing the work.
  + Implement change as scheduled documenting work as work is completed.
  + If the RFC creates an outage create an incident ticket and document the reason for outage and then fail the RFC as “**Failed with Ticket**.”
  + If the change failed but needs to be rescheduled to accomplish the desired result, close the change as “**Failed and Reschedule**.”
  + If the change failed and is no longer required, close the change as “**Failed and Close**.”
  + If the change is started and is no longer needed or back out close the change as “**Aborted**.” In Remedy, close the change as “**Cancelled**.”
  + If the RFC was completed with issue, close the RFC as “**Completed with issues and document the issues**.”
  + If the RFC was successful, close the RFC as “**Implemented Successfully**.”
* There shall be policies and procedures to control the implementation of ECRs.

## Post-Change Documentation and Reporting Policies

* All completed RFCs shall include execution and post-change documentation.
* The on-shift engineer acting as a change validator shall review all changes for success and post-change documentation.
* The change requestor shall document all steps in the change as an initial RFC requirement to ensure the assigned team understands how to validate the change after implementation.
* Change records shall be analyzed regularly to detect increasing levels of changes, frequently recurring types, emerging trends, and other relevant information.

## Policy Exclusions

### Hosting Dedicated Network Gear (Dedicated Customer Environment)

If a planned change cannot occur, the customer can request an expedited change on their dedicated network equipment. This type of change will still require a change request and a warm hand off to the Change Management team. However, the change should not require a peer review nor customer advocate approval (unless required by the customer) and should be assigned to the engineer requesting the change.

### Remote Application Management

Remote Application Management (RAM) changes are held to Service Level Agreements (SLAs) with the Client. At times, RAM changes must be handled in an expedited manner(Note). These changes still require SOC Validation and all change requirements. They just have to be executed in a more timely fashion. Thus, the required advance submission and emergency approval process is void for these types of change requests.

**Note**: “Expedited manner” allows for a two-hour turnaround from client approval to execution.

### Standard Changes

CAB requests for Standard Change events that are low risk, standardized where the risk and impact is documented, known, clearly understood and predictable are pre-approved. Standard Changes 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.

### Contractually-Excluded Products

Certain products are exempt from this policy due to specific change management standards laid out in their contract. All contractually-excluded product groups must have on a Policy Deviation Statement on file in Document Management System (DMS) that has been staffed through and approved by the Change Management department.

# Responsibility

The Cloud Governance and Compliance organization publishes policy, process, and procedure documents as a reference. The Verizon Business Owner (BO) or Information Resource Custodian (IRC) of record as defined by Verizon Corporate Security Policy is responsible and held accountable for enforcement of published policy, process, and procedure documentation.

It is the responsibility of all Cloud personnel to know, understand, and conform to the policies set in Verizon Corporate CPI-810, Verizon CPS-303, Verizon CPS-130, and others as they apply to all Verizon employees.

## 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 Verizon Counsel and coordinated with the responsible security executive for resolution.

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

## Management Commitment

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

This policy has been managed by [SECM-00089 Policy Management Process](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00089%20Policy%20Management%20Process.pdf) and approved by Verizon Cloud Information Security Council.

# Exceptions

Exceptions to this policy must be approved by the BO or IRC of record as defined by Verizon Corporate Security Policy.

# Expiration

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

# Enforcement

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

# Appendices

Appendix A - Terms and Definitions 9

Appendix B - Risk and Impact Assessment 12

Appendix C - RFC Submission Guidelines 13

Appendix D - OCRB and MASTARS Submission Guidelines 14

Appendix E - Maintenance Window Guidelines 15

Appendix F - References 16

Appendix G - Distribution 17

Appendix - Terms and Definitions

Table A‑: Terms and Definitions

| Term | Definition |
| --- | --- |
| BO | Business Owner |
| Break Fix | An Incident ticket that required an immediate remediation to restore a loss of service. The Break Fix on Verizon shared environment must require management level approval. |
| Change | Change as it pertains to Verizon Change Management is defined as any modification to fit, form, or function of a Verizon system or a system managed by Verizon. These systems include:   * Hardware * Software * Configuration of computers * Networks * Databases * Communications equipment * Any other component introduced into the Verizon 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 Verizon 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 |
| CISC | Verizon Cloud Information Security Council |
| Cloud | Verizon Enterprise Solutions (VES) Cloud and Data Center Services include all of the services Verizon provides to the customer within the cloud and connectivity solutions portfolio (e.g., all cloud offerings, managed hosting, colocation, etc.), as well as any Verizon organizations providing support for cloud and data center environments. |
| Client Advocate | Refers to the different ways clients are represented in Verizon . 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. |
| DC | Data Center |
| DMS | Document Management System |
| Emergency Change Request (ECR) | An RFC that needs to happen outside of standard maintenance window guidelines. |
| Executive Review Board (ERB) | The Verizon 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. |
| IRC | Information Resource Custodian |
| OCRB | The Organization Change Review Board is an internal Verizon team comprised of technical engineers that review facility maintenance activities for risk and impact prior to formal change submission. |
| 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. Verizon should receive advance notification to allow for customer notification and change documentation on the FSoC. |
| Personnel | All Verizon full and part-time employees, temporary workers, volunteers, contractors, or any other agents employed to perform work and who have been granted access to Verizon Cloud and Data Center Services information systems and information assets. |
| 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 Delivery 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 |
| SLA | Service Level Agreements |
| 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 | Verizon 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 |
| Unauthorized Change | A change made to the VZCS or customer’s IT infrastructure that violated defined and agreed upon Change policies. |
| VES | Verizon Enterprise Solutions |

Appendix - Risk and Impact Assessment

Every change has 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 RFC must be assigned one of the following risk categories:

Table B-: Risk and Impact Assessment

| Risk Level | Definition | Required |
| --- | --- | --- |
| 1 High | High potential impact to large number of users/customers or business-critical services because of the introduction of new product, software, topology, or feature; or because of a large increase of traffic or users, backbone changes, or routing changes; change involves expected service delivery (SD) impact.  **Note**: Level 1 changes require TPR and ERB approval prior to presenting to the CAB. All platform level updates are considered to be Risk Level 1 and must be tested and approved before being moved into the production environment. | Approval From: CAB/TPR/ERB/CMA  Attachments:   * Plan/Testing * Detailed Implementation Steps * Peer Review or SOC Validation |
| 2 Medium | Medium potential impact to a smaller number of users/customers or business services because of any non-standard change, such as upgrade or new product, software, topology, features, increased traffic, or non-standard topology; change may require some SD impact. | Approval From: CAB/ TPR/CMA  Attachments:   * Detailed Implementation Steps * Peer Review or SOC Validation |
| 3 Low | Low potential impact to multiple customers or impact to individual customer, including adding new standard template network modules (building or server switches, hubs, or routers); bringing up new wide area network (WAN) sites or additional proven access services; change or upgrade infrastructure applications or tools; and all risk level 2 changes that have been tested in the production environment. Change may require some network, server, or customer downtime. | Approval From:  CAB/CMA  Attachments:   * Detailed Implementation Steps * Peer Review or SOC Validation |
| 4 Routine | Pre-approved CAB (Standard) changes and routine activities that present no user or service impact to multiple customers, including adding individual users to the network, and standard configuration changes such as password, banner, Simple Network Management Protocol (SNMP), or other standard configuration parameters; Shared Network Changes, Changes for Managed Hosting clients and dedicated customer devices, no expected impact to shared network or possible impact to dedicated devices or shared Web/Structured Query Language (SQL) services, or RAM changes. | Approval From: CMA/ SM  Attachments:   * Detailed Implementation Steps * Peer Review or SOC Validation |
| 5 Standard | 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 Changes 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. | Approved From: CAB  Attachments:   * Detailed Implementation Steps * 3 Consecutive Successfully Implemented RFCs |

Appendix - RFC Submission Guidelines

RFCs that are submitted outside of the following posted timelines may be rejected, rescheduled, or require ECR submission.

* An ECR may be submitted for CAB/EC approval at any time. An ECR is only used when a situation arises, which is unplanned but critical in nature. An ECR is NOT to be used as a substitute for poor planning. Always follow up the ECR submission with a phone call to the **Change Administrator** on call and an email. The phone call should be made to **469-461-9348**. The email should be sent to the distribution list: **GRP Emergency Change Notification**.
* A planned RFC must be submitted with the minimum lead times as outlined below:

Table C-: RFC Submission Guidelines

| 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 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 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. * **MASTARS**: CAB level infrastructure RFCs must be submitted to allow for 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.

Appendix - OCRB[[1]](#footnote-1) and MASTARS[[2]](#footnote-2) Submission Guidelines

RFCs that are submitted outside of the posted timelines below may be:

* Rejected
* Rescheduled
* Require ECR submission

RFCs that are processed through the Organization Change Review Board (OCRB) are handled differently than other Verizon maintenance activities. The following list contains only high-level guidelines. Please reference the TMQM document [CHGM-00003 Facilities Operations Change Management Process Guide](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Service%20Delivery/Change%20Mgmt/CHGM-00003%20TQM%20Facilities%20Operations%20Change%20Management%20Process%20Overview_old%20template.pdf) for more detailed information regarding facilities changes.

* Facility changes will be assessed for Risk and Impact based on the facilities risk matrix. Based on the results of the facility risk matrix anything other than routine scores will require presentation to the OCRB.
* If a proposed change requires presentation to the OCRB, the OCRB will review the change and potentially adjust the score based on the concurring opinions of the OCRB.
* If the change scores a critical rating on the facilities risk matrix and is approved by the OCRB, it will be raised through the Verizon Change Management toolset for CAB review and approval.
* Pending a Verizon CAB approval, Verizon will then raise the change in Maintenance Activity Scheduling and Reporting System (MASTARS) for Global Event Notification and Management Center (GENMC[[3]](#footnote-3)) awareness and notification purposes only. This will occur if the CAB presents a direct impact to client operations and/or if there is a critical risk to continued normal operation as scored by the facilities risk matrix and validated by the OCRB.
* Risk levels are documented in the Change Management Policy, Appendix C, Table C-1, and are applicable for all OCRB-approved change submissions.
* Submission guidelines are documented in the Change Management Policy, Appendix C, Table C-1, and are applicable for all OCRB approved change submissions.
* Advance notification guidelines are documented in Section 2.5, and are applicable for all OCRB approved change submissions.

Appendix - Maintenance Window Guidelines

If these maintenance window guidelines cannot be met, CAB approval is required or the ECR process must be followed to gain Cloud VP/Director approval.

Table E-: Maintenance Windows Guidelines

| Maintenance Type | Maintenance Time | |
| --- | --- | --- |
| Major Infrastructure Maintenance Windows | Daily 00:00 – 06:00 | Local Data Center Time |
| **Note**: Submit ECR if required outside of these windows. | |
| Shared Network Maintenance Windows | Daily between 23:00 – 07:00 ET (GMT-4) | North and South America |
| Daily between 16:00 – 00:00 ET (GMT-4) | EU Shared managed in the US |
| Daily between 22:00 – 06:00 CET (GMT+1) | EU Shared managed in the EU |
| Daily between 22:00 – 04:00 JST (GMT+9) | APAC |
| **Note**: Submit ECR if required outside of these windows. | |
| Device Maintenance Windows | All dedicated changes will be scheduled in the customer-designated maintenance window (best effort or upon Client Advocate approval.) | |

Appendix - References

Table F‑1: References

| Document Number | Document Title |
| --- | --- |
| CHGM-00003 | [TQM Facilities Operations Change Management Process Overview](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Service%20Delivery/Change%20Mgmt/CHGM-00003%20TQM%20Facilities%20Operations%20Change%20Management%20Process%20Overview.pdf) |
| CPI-810 | Verizon Information Security Corporate Policy – Instruction  <https://vzweb2.verizon.com/learn-about-security-policies-cpi-810> |
| CPI-810 | 5.0 Operations Management  <https://vzweb2.verizon.com/sites/wireline/files/media/Operations%20Management.pdf> |
| CPS-130 | [Verizon’s Records Management](https://vzweb2.verizon.com/sites/wireline/files/media/upload/Corporate_Policy_Statement_cps_130_Records%20Management.pdf) |
| CPS-303 | [Verizon Protection of Customer and Employee Information](https://vzweb2.verizon.com/sites/wireline/files/media/upload/Corporate_Policy_Statement_cps_303_Protection%20of%20Customer%20and%20Employee%20Information.pdf) |
| CPS-810 | [Verizon Information Security Corporate Policy Statement](https://vzweb2.verizon.com/sites/wireline/files/media/Corporate_Policy_Statement_cps_810_Information%20Security%20Policy.pdf) |
| SECM-00089 | [Policy Management Process](http://mia21654sps460.apps.tmrk.corp:35214/Quality%20Management/Public%20Documents/Security%20Management/SECM-00089%20Policy%20Management%20Process.pdf) |
| Verizon Code of Conduct | <https://aboutyou.verizon.com/HRGuidelines/VzCulture/EthicsCompliance/CodeOfConduct> |

Appendix - Distribution

Table G‑1: Distribution Contacts

| Name/Role | Contact Information |
| --- | --- |
| TCC | [IT.Governance-TCC@one.verizon.com](mailto:IT.Governance-TCC@one.verizon.com) |
| CISC | [IT.Governance-CISC@one.verizon.com](mailto:IT.Governance-CISC@one.verizon.com) |
| Document Management | [Document.Management@one.verizon.com](mailto:Document.Management@one.verizon.com) |
| VZCS Change Management | [grpglobalchangemanagement@verizon.com](mailto:grpglobalchangemanagement@verizon.com) |
| Jeff Nord Global | [Nord.MSPE.Global.Org@one.verizon.com](mailto:Nord.MSPE.Global.Org@one.verizon.com) |

1. The OCRB is an internal Verizon team comprised of technical engineers that review facility maintenance activities for risk and impact prior to formal change submission. [↑](#footnote-ref-1)
2. MASTARS is a Verizon toolset utilized for raising, reviewing, approving, scheduling, and notifying of maintenance. [↑](#footnote-ref-2)
3. GENMC is a Verizon team that ensures the integrity of the enterprise. The vision and mission of the GENMC are:

   * Vision: Global providers of value-added information of network events that ensures the integrity of the enterprise.
   * Mission: To be reliable, knowledgeable, and timely facilitators of information regarding network events, and dedicated to providing concise guidelines and policies for safeguarding our clients and networks.

   [↑](#footnote-ref-3)