IT Management of Change Procedure (Technical, Physical and O&M)

SUMMARY

The Enterprise IT Change Management Process refers to managing changes in the IT environment (data, configuration, software, hardware). This procedure describes the steps to complete to ensure proper planning, impact assessment, testing, coordination, and approvals necessary to minimize the risk to production and business processes associated with implementing changes. All changes to PG&E IT production environments and systems are to be represented by a completed and approved CRQ (Change Request) in the Service Management Tool (SMC Remedy).

The requirements in this procedure are aligned with the PG&E Safety Excellence Management System (PSEMS) Element 10: Management of Change and GOV-4005S – Management of Change Standard.

TARGET AUDIENCE

PG&E employees, contractors, and vendors, temporary personnel, and other outside personnel, who initiate, approve, or deploy changes to PG&E IT production environments and systems.

SAFETY

Failure to follow the steps outlined in this procedure could result in missing a key step that completes the IT Change Management Process and could introduce risk into the organization.

BEFORE YOU START

The objective of this procedure is to outline the steps required to complete an IT Change request (CRQ) for application/system, supplier/contracts, and environmental changes.

WBT 2512 (Remedy Change Mgmt) and the ITSM SP Home page provide additional training and information. Link: ITSM Home - Home (sharepoint.com)

TABLE OF CONTENTS

IT Management of Change Procedure (Technical, Physical and O&M)

PROCEDURE STEPS

1 Initiate a Change Request (CRQ)

1.1 Create CRQ in Remedy.

NOTE

Remedy is the system of record for all IT Change Requests (CRQs). All production changes must be logged in Remedy, fully approved, and scheduled before being implemented in any production environment.

1.2 SELECT class of IT Change.

Type or Class of Change	Description	Level of Approval
Normal Class	A non-standard, non-emergency change to production environments/systems.	This change class requires a complete change review process including Change Advisory Board (CAB) approvals. Change Owners are to plan accordingly for CAB lead times.
Emergency Class	An unplanned and unforeseen change that requires immediate assessment and implementation to restore a service or prevent disruption to production environments/systems. Such changes have a major business impact if not implemented.	Changes that are elevated risk are approved by eCAB members; the active incident commander, the accountable service/product owner, and the impacted key stakeholder(s) of the service/product. The respective Domain CAB approves lower risk changes

IT Management of Change Procedure (Technical, Physical and O&M)

Expedited Class	A change that is not classified as either an Emergency or Normal class and must be implemented without waiting for the next scheduled CAB meeting. These changes require accelerated implementation due to implications related to employee/public safety, regulatory commitments, compliance, or fines.	Approvals for Expedited Class Changes: • Changes that are fully within the authority of the DCAB and less <2.49 risk score will require an expedited approval from the implementing team senior accountable leader, the impacted platform/system senior accountable leader and the DCAB. • Changes that are not fully within the authority of the DCAB and/or >=2.49 will require an expedited approval from the implementing team senior accountable leader, the impacted platform/system senior accountable leader and the TCAB.
Standard Class	Include routine activities that affect an application software and/or hardware device (i.e., configuration items) with well-understood implementation and backout procedures. They are low risk, low impact, non-outage changes, typically operational or maintenance in nature.	Changes are pre-approved, which means the system owners and business owners (if SOX) of the Configuration Items (CI) have agreed there is no need for formal review and approval every time a request to perform the work in initiated or received.
Dev-Sec-Ops Class	Framework to ensure Change Requests and Pull requests from teams that do not use Remedy are synchronized with Remedy for ENOC Visibility.	Approvals built into process
Jira	JIRA for approved Systems of Innovation (standard change class) for some teams that specific work processes.	Approvals built into process

1.3 COMPLETE all Minimum requirements for production IT Changes:

- Concise executive change summary
- Clear outage and impact assessment details (time/date/location/App)
- Method of procedure (MOP) – steps team will take during implementation.
- Backout plan (BOP) – measured & tested roll back procedure steps.
- Complete all risk scoring assessment questions.
- Evaluate plan/ results – include details about testing or attach URL to CRQ

IT Management of Change Procedure (Technical, Physical and O&M)

- Line of business approval for all key stakeholders
- Outage window – detail time & date of outage
- Post implementation Validation (PIV)

1.4 See **Appendix A** - IT Change Process Flow Diagram, **Appendix B** - Change Process Workflows in SMC and **Appendix C** – Roles and Responsibilities for more details.

2 Conduct Risk Assessment

2.1 ANALYZE IT Change risks.

2.2 DETERMINE appropriate mitigation actions.

2.3 REVIW 5MM CRQ Scoring to calculate business consequences if the intended mitigation controls do not prevent significant errors during the clearance.

NOTE
Risk scoring is a guide, not an exact science. Scores are to be based on the business consequence.

2.4 COMPLETE IT Change risk scoring questions to determine the risk level and if any additional approvals are needed.

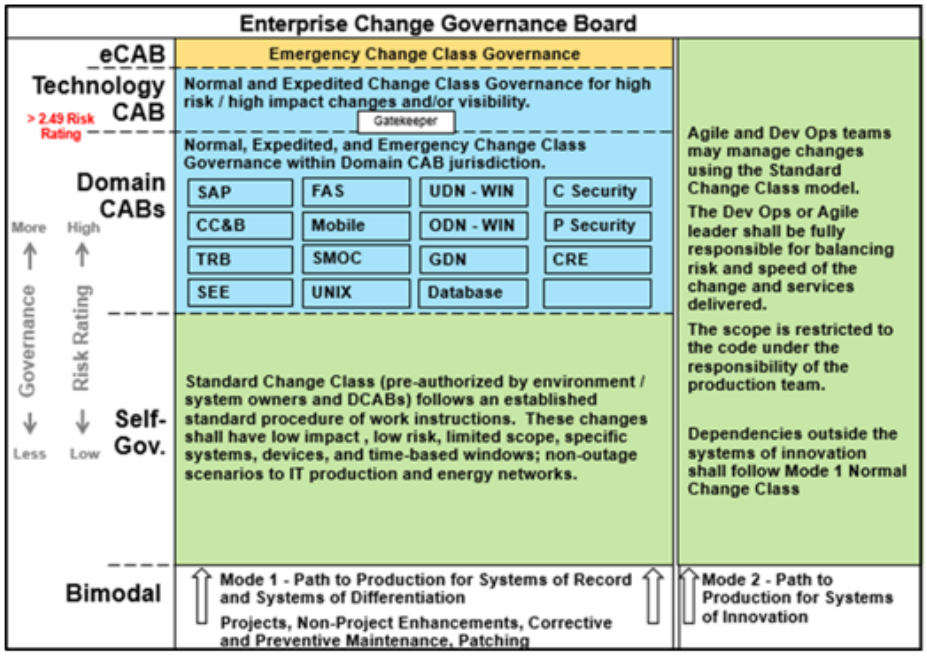
2.5 For CRQs with a risk **(2.49 or below),** SUBMIT to DCAB (Domain Change Advisory Board) for the review, compulsory risk assessment, approval, maintenance, and audit of standard class changes within their respective domain.

2.6 DCAB, REVIEW, ASSESS, and APPROVE normal class changes prior to submittal to Technology CAB or other domain CABs.

2.7 For CRQs with a risk **(2.49 or above),** SUBMIT to TCAB (Technical Change Advisory Board) for review and approval.

2.8 TCAB, REVIEW, ASSESS and APPROVE elevated risk normal class and expedited class changes that post an elevated risk of service disruption or negative impact to the business or customers. **See Figure 1** for Change Advisory Board (CAB) Structure & Relationships.

Figure 1 – Change Advisory Board (CAB) Structure & Relationships



3 Stakeholder Review & approval

Segregation of Duties

Segregation of duties (SOD) is applicable as a requirement to all change requests under change management control. Segregation of duties addresses the risk of malevolent activity without collusion, negligent or deliberate system misuse, due to abuse of authorized privileges.

A waiver from segregation of duties may be given to specific applications/systems based on risk, impact, and operational resource/staff availability. All such waivers are to be granted in writing by the IT Change Management Process Owner and may require concurrence from the Internal Audit Team for security and compliance.

IT Management of Change Procedure (Technical, Physical and O&M)

The following key segregations of duty are to be maintained.

Change Requester	Must not be the Independent Tester, Change Peer Reviewer, or Change Approver
Change Coordinator	Must not be System Owner, Peer Reviewer, or Independent Tester
Change Peer Reviewer	Must not be the Change Requester, Independent Tester, or Change Approver
Independent Tester	May be the System Owner or Line of Business
Change Implementer	Must not be the Independent Tester, Peer Reviewer, or Change Approver
Change Manager	Must not be the Change Requester, Independent Tester, Peer Reviewer or Change Approver
Change Approver	May be the System Owner, ENOC, or Line of Business
May be the System Owner, ENOC, or Line of Business	May be the Change Approver, Line of Business

NOTE

Each change/clearance must have three roles: Change Requester, Change Peer Reviewer and Change Approver – ALL ARE TO BE DIFFERENT PEROPLE.

3.1 IDENTIFY TCAB & DCAB Change approvers and notifications recipients by the configuration items, circuits. Systems, applications, devices, and networks impacted by the change.

3.2 ASSOCIATE Approvers with the individual configuration items impacted and auto pulled or entered into the change record in the CRQ as a required approval.

3.3 REVIEW CABs technology, process and Standard Operating Procedures (SOP) LINK: DCABChangeManagementSOP.docx

3.4 EVALUATE, REVIEW and APPROVE production changes per SOP.

4 Communication Plan

All outage Changes must be communicated with IT to ensure the change is acknowledged and approved.

NOTE

Change Implementers CANNOT move forward with an application change until IT Stakeholder approval is obtained.

4.1 Change Implementers, Managers and lifecycle project managers, COORDINATE communications with TSC Communications Team for impactful production changes to all key stakeholders.

4.2 TSC Communication Team SEND targeted CRQ announcements to key stakeholders. CRQ Comms Matrix: Communications Matrix 2020.xlsx (sharepoint.com)

IT Management of Change Procedure (Technical, Physical and O&M)

5 Testing and Verification

Application Owners and Change Implementers are responsible to test changes before scheduling a change in production environment(s). This must be completed and documented before a CRQ is presented for approval or scheduled for production.

5.1 TEST changes in lower environment to reduce risk associated with changes that cause production incidents.

IF you do not have the capability to evaluate changes

THEN

ENGAGE the Testing Center of Excellence (TCOE) Team (for applications) or Enterprise Architecture Team (for hardware issues).

NOTE

IT Change Team does not possess the technical skills to audit testing.

5.2 DOCUMENT testing.

5.3 ATTACH to CRQ before submitting for approval.

6 Production IT Change Implementations

6.1 CALL (415) 973-3662 or EMAIL ENOC Operations to start and complete production CRQs.

6.2 NOTIFY affected upstream/downstream system owners of change window.

6.3 For critical data center work, SCHEDULE and OPEN a bridge call.

6.4 INVITE ENOC Operations for large scale CRQs (FFIOC/RCIOC/Control Centers activities).

6.5 ENSURE IT operational teams are on standby in the event of unexpected technical issues.

NOTE

ENOC can be used to escalate requests to the technical teams during production incidents.

IT Management of Change Procedure (Technical, Physical and O&M)

7 Post Implementation & Validation

7.1 All change submissions must have a post-implementation validation plan that identifies all required line of business and application owner signoffs to close out the CRQ. Teams/technicians are not to be released from the CRQ until this last step is completed. The formal signoffs are to be enforced at the submission of the change for processing point, Peer, and Supervisor review, and at the Domain CAB review.

Project Managers/ENOC also need to enforce the completion of this step in post-implementation activity directly after the change and prior to the close-out of the CRQ. Any change that is deemed as less than successful or failed is to launch the Post Implementation Review (PIR).

The change manager of the CRQ is responsible for coordinating a Post Implementation Review (PIR) on CRQs with the following conditions: a change that created an unknown/unexpected impact; a change that failed; a change that was not effectively communicated; or a change with further impact than indicated from the review process.

8 Change Completion & Documentation

Change Implementers are responsible to document and complete all production changes (within 48 hrs of change) based on the change outcome, successful or unsuccessful. LINK: CRQ Close Out & Safety Procedure

8.1 DOCUMENT completion

8.2 CLOSEOUT CRQ.

9 Effectiveness Review

Effectiveness is determined during post validation within the timeframe of completing the CRQ. Change Owners conduct the review.

9.1 CONDUCT review of the effectiveness of the change.

9.2 DOCUMENT results.

9.3 REFER to CRQ document as reference.

End of Requirement

DEFINITIONS

N/A

IT Management of Change Procedure (Technical, Physical and O&M)

IMPLEMENTATION RESPONSIBILITIES

Infrastructure and Operations Sr. Manager or assigned delegate will ensure access to this procedure is provided and communicated to the employees qualified to complete the associated tasks.

Infrastructure and Operations Sr. Manager or assigned delegate will ensure access to this procedure is provided and communicated to other relevant lines of business for distribution within their organizations.

Managers and Supervisors with employees who perform the steps provided in this procedure will ensure work is completed as specified.

Employees who perform tasks specified in this procedure are responsible for complying with the steps provided.

GOVERNING DOCUMENT

GOV-4005S Enterprise Management of Change Standard

COMPLIANCE REQUIREMENT / REGULATORY COMMITMENT

Information and Records Management:

PG&E Data, Information, and Records are company assets that must be traceable, verifiable, accurate, and complete and can be retrieved upon request. Functional Areas are responsible for complying with the Information & Records Governance Policy, Standards, and the Information and Records Retention Schedule. Refer to GOV-7101S, “Enterprise Records and Information Management Standard” for further guidance or contact Information & Records Governance at Information&RecordsGovernance@pge.com:

REFERENCE DOCUMENTS

Developmental References:

N/A

Supplemental References:

N/A

APPENDICES

Appendix A – IT Change Process Flow Diagram

Appendix B - Change Process Workflows in SMC

Appendix C – Roles and Responsibilities

IT Management of Change Procedure (Technical, Physical and O&M)

ATTACHMENTS

N/A

DOCUMENT RECISION

N/A

DOCUMENT APPROVER

Joe Le, Director, Enterprise Operations

DOCUMENT OWNER

Jason Magee, Senior Manager, Infrastructure & Operations

DOCUMENT CONTACT

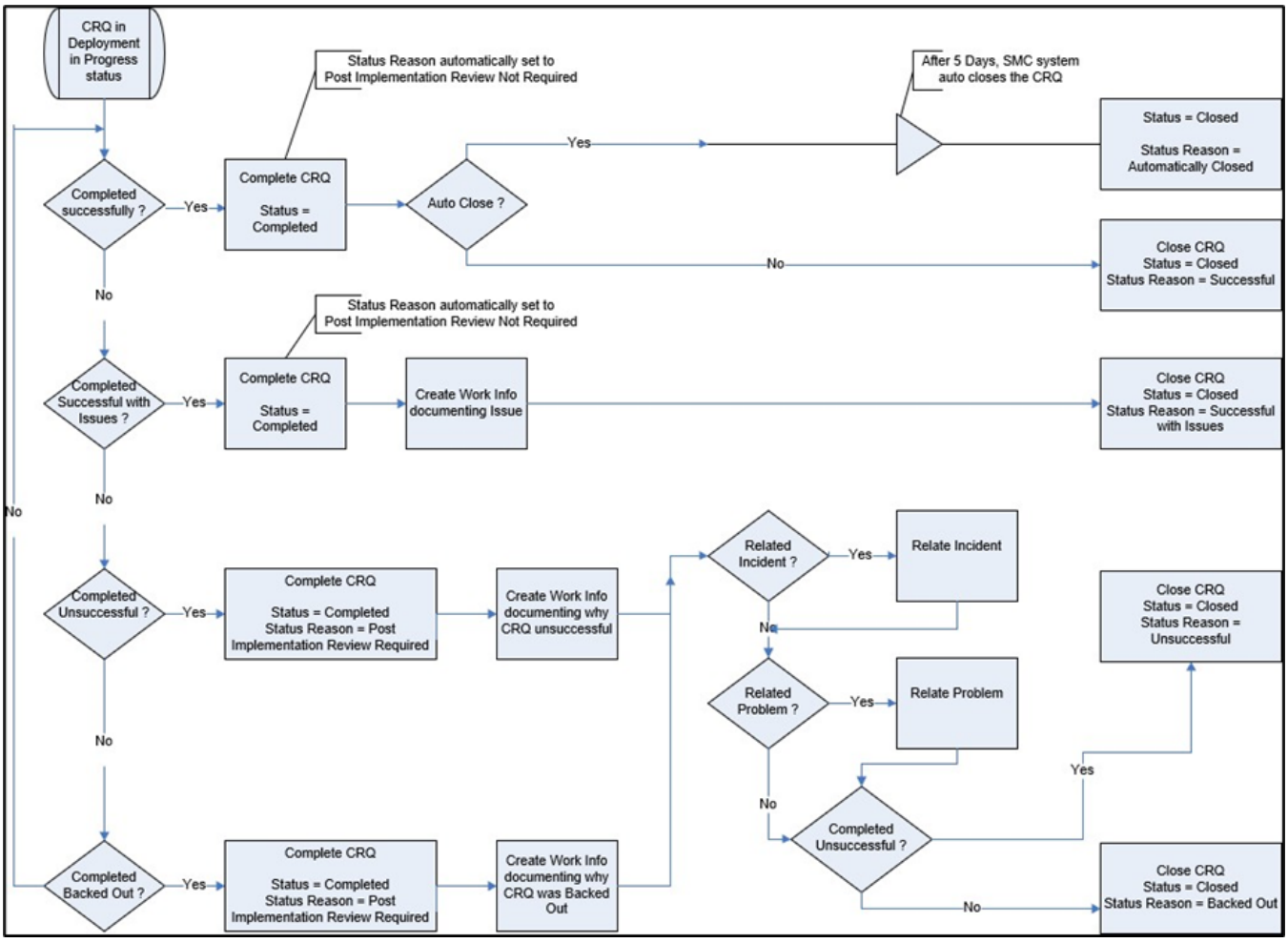
Kenny Key, Product Owner, Principal

REVISION NOTES

Where?	What Changed?
Entire Document	New Procedure See EDRS 2024-40346 for Approvals

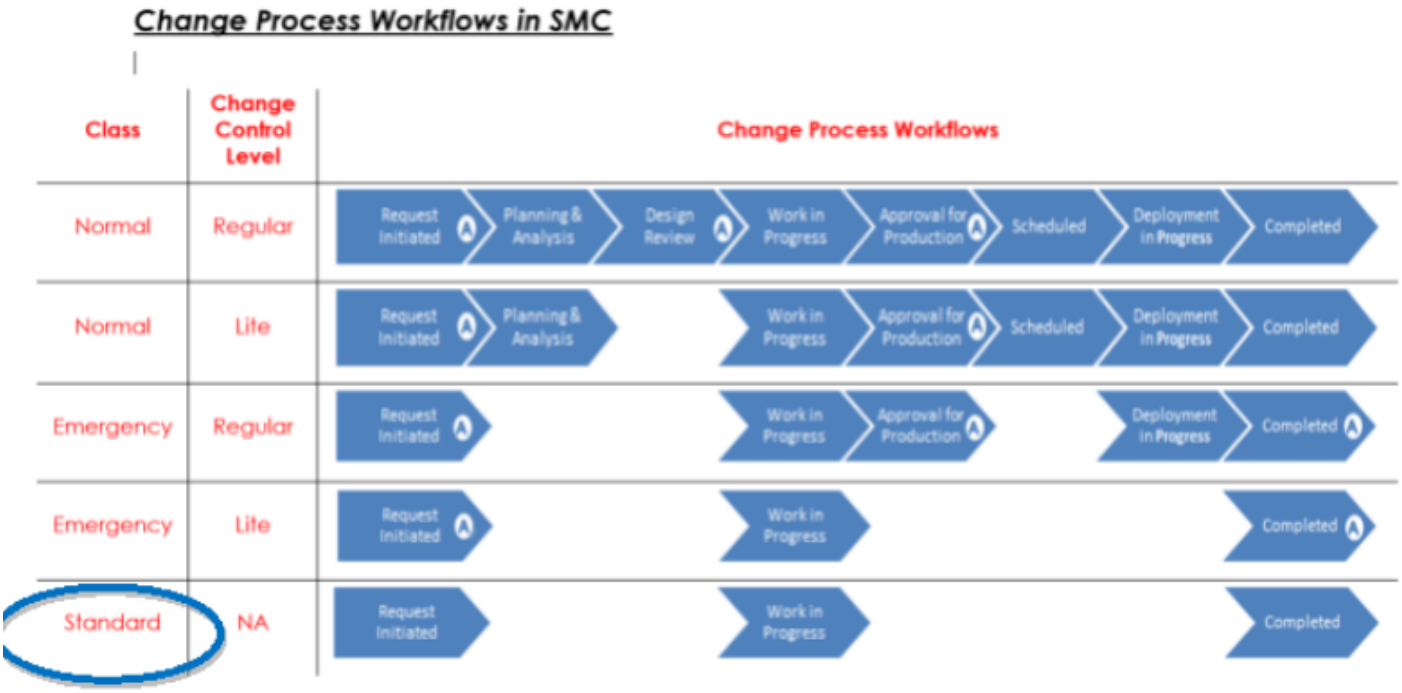
IT Management of Change Procedure (Technical, Physical and O&M)

Appendix A, IT Change Process Flow Diagram
Page 1 of 1



IT Management of Change Procedure (Technical, Physical and O&M)

Appendix B, Change Process Workflows in SMC
Page 1 of 1



IT Management of Change Procedure (Technical, Physical and O&M)

Appendix C, Roles and Responsibilities

These tables below set forth the roles and responsibilities required by the Enterprise Change Management Process.

Role	Responsibility
Change Management Process Owner	1. Overall responsibility for the IT Change Management process and its adoption company wide. 2. Review all updates and changes to the IT Change Management Standard, Process, and/or tools to ensure compliance with existing regulations and industry best practices.
Change Management Process Manager	1. Oversee the implementation of PG&E's IT Change Management Standard, establish compliance monitoring and reporting, guide the coordination activities for Change Advisory Boards (CABs). 2. Periodically test the Change Management process for adherence and report on the results to management.
Change Requester	1. Define and document business justification and nature of defect (if applicable) for change in the Request for Change Form. 2. Complete all necessary information pertaining to the request as specified by the Request for Change Form. 3. Submit the Request for Change Form for approval to the Business Owner.
Subject Matter Experts (Developer/Technician/Engineers / Specialist)	1. Responsible for technical build-out review of the CRQ as presented. 2. Responsible for identification and classification of technical risk – critical to the risk and impact analysis for the change. 3. May be required to present the CRQ to the DCAB / TCAB if the CRQ is technical in nature and the submitter is not able to accurately represent the change. 4. Participate in in post-change analysis on any change resolved less than successfully.

Role	Responsibility
Change Coordinator (typically Team or Technical Lead or submitter team)	1. Gather the CRQ artifacts. 2. Review and pre-screen the business justification of Requests for Change. 3. Review risk and impact analysis and make changes as appropriate. 4. Notify parties of Request for Change status and facilitate updates to or cancel Requests for Changes that are not approved. 5. Provide Notification of approval for installation to production and / or for Implementation of Back out Plans. 6. Coordinate personnel assignments and workflow. 7. Ensure all required documentation for the submission of the request for change is completed; return incomplete requests back to the requester for additional information required. 8. Work with the Change Builder and System Owner to ensure appropriate updates to technical documentation and training procedures where appropriate and facilitate end-user notification of procedure changes and training needs. 9. May be required to represent the CRQ at the DCAB / TCAB if required by risk factor score (See ITS5500- MP01) 10. Close completed changes in a timely manner *Note: There may be multiple Change Coordinators for a system.*
Change Manager (typically a supervisor)	1. Monitor change requests to ensure they are being completed in a consistent and timely manner. 2. Ensure process compliance within application/system support group. 3. Review reports provided by Change Coordinator 4. Represent the CRQ at the CAB if required by risk factor score. 5. Approve the change prior to TCAB as the local change authority.

IT Management of Change Procedure (Technical, Physical and O&M)

Role	Responsibility
Change Peer Reviewer	Ensure that: 1. The work is technically sound, tested and represented correctly on the change in business-friendly language 2. All configuration items, circuits, systems, devices, networks impacted/affected items are identified 3. Testing has been completed and the results are included in the change documentation 4. A detailed method of procedure (MOP) is included, and Back Out Plan is provided 5. Related Tasks/Work Orders/Service Requests are assigned and associated to the change request 6. Lead time is adequate for the change as requested 7. Requested change date/time does not adversely affect other systems/client's work 8. Risk and impact have been correctly assessed (See Appendix Priority Matrix) 9. Project accounting (order numbers) submitted are valid and will remain open until the work is completed (when required) 10. All business clients affected are identified 11. Subject matter experts (SMEs) are identified, if required, 12. Technical or ITCAB Review(s) is/are indicated if necessary 13. Any additional approvals or notifications, if required, are obtained (LOB, Project Managers, etc.) 14. Peer review approval granted

Appendix C, Roles and Responsibilities
Page 4 of 6

Role	Responsibility
Change Implementer (also known as Change Builder)	1. Perform risk and impact analysis assessing and categorizing change. 2. Develop design. 3. Build/Modify change, create back out plans, conduct unit testing, determine feasibility. 4. Document unit testing procedures. 5. Retrieve the source code from the production source code repository when modifying programs. 6. Conduct initial unit testing and determine feasibility of the Change. Document justification if the Change is not feasible and provide alternative solutions where applicable. 7. Document unit test procedures. Provide test results to the CRQ. 8. Perform necessary technical preparations for the change. 9. Document (or obtain from users) problems noted during the testing processes, make appropriate modifications in the development environment, and submit modifications to the Independent Tester for retesting. 10. Communicate / provide notification of test results for final approval. 11. It is a good practice to Notify ENOC when starting, completing, and / or requesting an extension of the change/clearance window, and cancelling change(s) to production. 12. Update Technical documentation where appropriate. 13. Update Training procedures where appropriate. 14. Complete Code Migration form (if applicable). 15. Document technical specifications or system specifications for New or Enhancement changes.
Emergency Change Advisory Board	1. Emergency change justification is accepted as valid. 2. Review and approve Emergency Changes 3. Require post implementation review step and lessons learned and post implementation stabilization testing and sign off.
Business Owner / Business Approver (Key Stakeholders)	1. Review and approve business justification for change. 2. Identify issues and/or potential issues with a change and work with the System Owner to resolve these issues. 3. Review and approve risk and impact analysis. 4. Approve requests for change for an application for which he/she is responsible for. 5. Review and approve business requirements, design, and test plans. 6. Review and approve completed request for change and approve move to production. *Note: The appropriate Business Owners (Key Stakeholders) and sponsors may differ by system. Business Owners are identified by the System Owner, in conjunction with the Change Coordinator.*

IT Management of Change Procedure (Technical, Physical and O&M)

Appendix C, Roles and Responsibilities
Page 5 of 6

Role	Responsibility
System Owner / IT Approver (typically Manager or Supervisor)	1. Accountable for all changes to their respective system area (CI). 2. Review and approve risk and impact analysis. 3. Resolve request for change issues identified by the CAB and/or Business Owners. 4. Review and approve RFC to move to production. 5. Conduct post implementation reviews if needed and facilitate/ produce change management compliance reporting. (See Section KPIs) 6. Ensure IT staff receives appropriate training in change management process. 7. Establish and manage processes to provide appropriate revisions of the operations, user, and maintenance procedures for the CI. 8. Responsible to author, approve and audit Standard Changes for their area. Change audits an approval is required yearly.
Tester / Operations Staff	1. Coordinate all testing and reporting on test incidents and test results in the test environment. 2. Create Test Plans and test acceptance criteria as required. 3. Document testing procedures. 4. Install the request for change in the test environment. 5. Document the test results in the request for change to include any problems noted during testing. 6. Verify the change in production and update the request for change Form. *Note: Verification of the Change in production may be delegated to the requester, business owner etc.* *Note: Exceptions may be made for circumstances where testing is not conducted by the Independent Tester (or associated Testing Entity) and/or is delegated to another role. These exceptions must be documented and approved by the System Owner.*
Release Engineer (person responsible for managing the release)	1. Issue and maintain the change schedule. 2. Install an approved request for change by following the approved procedures at the designated time. 3. Install the request for change in the Production Environment. 4. Implement Back-out Plans for a Change as needed upon notification. 5. Notify ENOC if any unauthorized deviations from the baseline. 6. Monitor Request for change process.

Appendix C, Roles and Responsibilities
Page 6 of 6

Role	Responsibility
TCAB Chair (Technology CAB Chair)	1. Responsible for oversight of the TCAB meetings. Each in-scope change request will be reviewed during the scheduled CAB meeting. 2. Review each Change for risk and potential calendar conflicts. 3. Has the authority to ask that a change be rescheduled due to environmental issues e.g., other conflicting changes, network stability, weather events, incomplete documentation, incomplete testing, or missing approvals. 4. Ensure recording of Meeting minutes, attendees, and exception for each meeting, ensure storage on a shared location so any PGE Leader or other interested PGE party can view the results of each meeting.
Change Gatekeeper (TCAB Business Process Specialist)	1. Responsible for the quality control and completeness of the information contained in the CRQ. 2. Review the submitted information for completeness and ensure that all required documentation, proper lead times and Domain CAB or LOB approvals are present on a change record before formal TCAB review. 3. If upon review the submitted documentation is not reasonable (based on the complexity of the change, or information other controls or required documentation is missing) return the change to the Submitter/Requester for additional information.
Domain CABS/Change Approvers/Notification Recipients	1. Domain CABS, Change Approvers/Notifications are to be determined by the configuration items, circuits, systems, applications, devices, and networks impacted by the change. 2. Approvers are to be associated to the individual Configuration Items impacted and auto pulled or entered into the change record in the CRQ as a required approval. 3. Identified System Owner and LOB approvals are required for all changes.