CHANGE MANAGEMENT POLICY

April 2019

Table of Contents

1. SPONSOR ACCEPTANCE 3
2. OBJECTIVE AND POLICY OVERVIEW 4
3. KEY DEFINITIONS 5
4. CHANGE MANAGEMENT PROCESS 7
4.1. PROCESS OVERVIEW 7
4.2. PROCESSES 8
5. POST IMPLEMENTATION REVIEW 18
5.1. PROCESS 18
6. KEY PERFORMANCE INDICATORS 20
7. CHANGE MANAGEMENT APPROVAL 21
7.1. ENTERPRISE CHANGE CONTROL GROUP (ECCG) 21
7.2. VERTICAL CHANGE CONTROL GROUP (VCCG) 22
7.3. EMERGENCY CHANGE MANAGEMENT APPROVAL 23
8. Addendum A – NORMAL/HIGH PRIORITY CHANGE MANAGEMENT PROCESS 24
9. Addendum B – STANDARD CHANGE MANAGEMENT PROCESS 25
10. Addendum C – EMERGENCY CHANGE MANAGEMENT PROCESS 26
11. Addendum D – REQUEST FOR CHANGE (RFC) 27
12. Addendum E: OTS STANDARD OPERATING PROCEDURE (SOP) TEMPLATE 31
13. Addendum F: OTS SCHEDULE OF CHANGES TEMPLATE 32
14. Addendum H – CHANGE CONTROL GROUP MEETING MINUTES EXAMPLE 33
15. Addendum I – ROOT CAUSE TEMPLATE 34
16. Addendum J – RFC SUBMISSION PROCEDURE DIAGRAM 35

1. SPONSOR ACCEPTANCE

Approved by:

_____ Date: _____

Richard "Dickie" Howze
State of Louisiana – CIO

2. OBJECTIVE AND POLICY OVERVIEW

The objective of Change Management is to ensure that standardized methods and procedures are used to enable beneficial changes, while ensuring efficient and prompt handling of all changes to services provided by Office of Technology Services (OTS). The primary goals of Change Management are to minimize the disruption of services, reduce back-out activities, and ensure clear communication across IT and its customers.

In order to achieve this objective, OTS has defined the Change Management Policy as defined and described in this document with key tenets as follows:

- All changes to any OTS provided service are managed and approved through the Change Management process, regardless of source or type.
- The decision to authorize or reject a proposed change is based on the completed Change Management Process, to include proper understanding of the risks associated with the implementation of the change.
- Each type of change [Standard, Normal, and Emergency] will have specific submission, approval and execution requirements within this policy, including the specific levels of authorization and communication required for each type of change and all rules for assessing and executing Changes.

3. KEY DEFINITIONS

Change: A Change is defined by an addition, modification, or removal of configuration item that could have an effect on IT Services and which is approved by management, enhances business process changes (fixes) and minimize risk to IT Services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

Change Management: Change Management refers to the process used to control the lifecycle of all changes.

Change Management Policy: Change Management Policy is the guiding standard that describes the procedures for, and specifies the rules and levels of authorization required to approve, different types of Changes.

Change Proposal: A Change Proposal describes a proposed major Change, like the introduction of a new service or a substantial change to an existing service. The purpose of Change Proposals is to communicate a proposed major Change and assess its risk, impact and feasibility before design activities begin.

Change Record: A Change Record contains all the details of a Change, documenting the lifecycle of a single Change. It is usually created on the basis of a preceding Request For Change.

Compliance (Change) Managers: A Compliance Manager/Change Manager is the person that is responsible for ensuring that changes within their scope are managed from inception through presentation and into implementation. The scope of a compliance manager is either Enterprise focused or Vertical focused.

Configuration Item (CI): A Configuration item is any component or service that is managed in order to deliver an IT service. These include IT services, hardware, software, process documentation, and service level management.

Data Governance Influence Group (DGIG): The Data Governance Influence Group provides guidance and recommendations on the efficient, effective, and secure management and use of the State's information assets. Charged with developing and approving statewide data management policies and standards and promoting data sharing opportunities where possible. The DGIG is chaired by the State Chief Data Officer and consists of multiple agency Undersecretary level positions from agencies that own sources of data.

Emergency Change: An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs).

Enterprise Change Control Group (ECCG): The Enterprise Change Control Group is charged with overseeing the Change Management process for each Change and executing enterprise level change decisions. The OTS Portfolio Deputy Director will chair with Enterprise Governance Architect as co-chair with a unanimous decision voting method.

Information Services Influence Group (ISIG): The Information Services Influence Group is the joint OTS leadership and Executive Branch agency leadership group that is tasked with providing leadership around the State's ability to pursue and support IT excellence and gather a representative IT portfolio of project and service needs from all areas of the State. The ISIG is chaired by the Deputy CIO and consists of multiple agency Undersecretary level positions.

Maintenance Window: A Maintenance Window is a period of time designated in advance by the technical staff, during which preventive maintenance that could cause disruption of service may be performed.

Normal Change: A Normal Change is a change that does not have a pre-approved SOP and is not classified as an Emergency Change; it follows the full Change Management Process and have a predefined maintenance window.

Release: A set of new, changed and/or unchanged Configuration Items that are tested and introduced into OTS environments together to implement one or multiple approved Changes.

Remediation Plan: Remediation Plans are actions taken to recover after a failed change into production. These plans are required as part of the Release Management process and clearly defines the steps necessary to restore services to its previous level.

Request for Change Form (RFC): The Request For Change (RFC) is a formal request for the implementation of a Change. An RFC records the details of a proposed Change and must be submitted to Change Management process by the requestor for every non-Standard Change. The document will provide details of the change for approval and prioritization, and a mechanism for ECCG to govern the Change Management process.

Service Owner (SO): The role that is accountable for the delivery of a specific IT Service. OTS vertical directors (AppDM, CTO [EA], DCO, EUC, InfoSec, and PSS) are the Service Owners for all IT services offered by OTS. Service Owners can delegate decision making for services to leaders within their verticals as needed.

Standard Change: A Standard Change is a pre-authorized change that is low-risk, predictable in its outcome and repeatable through defined work instructions in a standard operating procedure (SOP).

Vertical Change Control Group (VCCG): The Vertical Change Control Group is responsible for the oversight of changes to production environments that are not enterprise level changes.

4. CHANGE MANAGEMENT PROCESS

Objective: The objective of this process is to govern the introduction of a change into production by insuring that the correct procedures are being followed, proper documentation has been completed, proper testing has been performed, and proper approval is in place.

4.1. PROCESS OVERVIEW

The Change Management Process is initiated as a result of a Service Request or as input from Project Management, Release and Deployment Management, or Incident and Problem Management. In turn, the Change Management process can provide input to other processes such as Project Management, Incident/Problem Management and Service Strategy; the latter through updates to the Service Catalog, policies and processes and/or Standard Operating Procedures (SOPs).

In order to accommodate different priority and impact levels, the Change Management Policy defines three (3) change types (Standard, Normal, and Emergency) and four (4) release types (Standard, Normal, High Priority, and Emergency)

- **Standard Change/Standard Release** – A Standard Change is a pre-authorized change that is low-risk, predictable in its outcome, and repeatable through defined work instructions in a standard operating procedure (SOP). SOPs for Standard Changes are reviewed by the Service Owner, pre-approved by the Vertical Change Control Group upon delegation by the Enterprise Change Control Group and are ready to use by technical Subject Matter Experts (SMEs) without further approval at the time of the change request. The body of SOPs will grow over time as OTS encounters repeat situations and develops standard procedures to handle these occurrences.
- **Normal Change/Normal Release –** A Normal Change is a change that does not have a pre-approved SOP, not classified as an Emergency Change, and can be implemented during predefined maintenance windows. Normal Changes follow the full Change Management Process. In general, all Service Requests, inputs from Project, Release and Deployment Management, and resolutions for low to high priority incidents in Incident and Problem Management, are handled as Normal changes.
- **Emergency Change/Emergency Release –** An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs). Emergency Changes will follow an abbreviated process and must be accompanied by a Post Implementation Review with Root Cause Analysis. All resolutions for major and critical incidents follow the Emergency Change process.
- **High Priority Release –** A high priority release is a business driven request for a release of a normal change (i.e. that does not have a pre-approved SOP, is not classified as an Emergency Change) and requires implementation outside of a standard maintenance window but not during operating hours (as with an Emergency Change). As with a Normal Change, a High Priority Release follows the full Change Management Process.

Each change type includes prescribed standards related to request, initiation, documentation, communication, testing, approval, and post implementation reviews as detailed below. The Request for Change (RFC) submittal procedures are detailed in Addendum J.

4.2. PROCESSES

Standard Change: All Standard Releases are governed by the pre-approved Standard Operating Procedure (SOP). This SOP must be reviewed by the Service Owner and approved by the Vertical Change Control Group.

1. Establish a Standard Change

1.1. In order to establish a Standard Change:

1.1.1. A Standard Operating Procedure must be drafted.

1.1.2. The change must have been successfully implemented in the past as outlined in the drafted Standard Operating Procedure.

1.1.3. The change must be repeatable, and its outcome predictable, as outlined in the drafted Standard Operating Procedure.

1.2. Once drafted, the Standard Operating Procedure must be presented to Service Owner for review and then to the Vertical Change Control Group for approval via email.

1.3. If approved, the Standard Operating Procure is published in the approved document library and the change is labeled as "Standard".

2. Standard Change(s) Deployment Approval

2.1. Standard Changes do not require approval by the Vertical Change Control Group but are required to provide notification.

2.1.1. All Standard Changes must be completed in a time frame approved by the Service Owner

2.1.2. If no approved Standard Operating Procedure exists, the change must follow the Change Management Process for a Normal or High Priority Change until requirements to "Establish a Standard Change" are completed.

2.2. Where possible, multiple Standard Changes should be released together and documented in a Schedule of Standard Changes.

2.2.1. The Schedule of Standard Changes should outline all changes to be released during the same window as well as details of the timing for that window.

2.2.2. Even if only one Standard Change is to be completed, a Schedule of Standard Change must be created and communicated.

2.2.3. A Change Item must be created in the official IT service management ticket solution and the Schedule of Standard Changes must be included in the ticket entry.

2.2.4. The Change ticket entry must have the following fields populated:

2.2.4.1. Request Type

2.2.4.2. Classification

2.2.4.3. Change Scope

2.2.4.4. Subject

2.2.4.5. Description

2.2.4.6. Contact

2.2.4.7. Priority

2.2.4.8. Notification

2.2.5. A Completed Request For Change (RFC) form must be attached to the ticket entry (see addendum D for template) until digital signatures are implemented

2.3. Once drafted, the Schedule of Standard Change will be sent via the service owner approved communication plan to service subscribers/consumers

2.4. If no issues or concerns are raised, release of changes may proceed as outlined in the Schedule of Standard Changes. Else, all outstanding issues and concerns must be resolved prior to execution of the change.

3. Deployment to Production

3.1. At the start of the change window communicated via the Schedule of Standard Changes, the assigned technical SME will communicate via the service owner approved communication plan to service subscribers/consumers notifying recipients that the change window is about to begin.

3.2. The assigned technical SME will then execute the approved SOP(s) for all changes planned in the Schedule of Standard Changes.

3.3. The technical SME will test each change per the established SOP for each in order to ensure that the desired expectations are met.

3.3.1. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue.

4. Successful Deployment

4.1. Upon a successful implementation of the change, the technical SME will communicate via the service owner approved communication plan to service subscribers/consumers notifying recipients that the changes are complete.

4.2. The Change Record will be updated to reflect successful completion of the Schedule of Standard Change.

5. Failed Deployment

5.1. If during the release, one or more of the changes results in a disruption of service or service level, an Incident must be created and the Incident Management Process must be followed.

5.2. Once resolved and the changes completed, a Post Implementation Review and Root Cause Analysis must be completed and attached to the appropriate ticket item.

5.3. Standard Operating Procedures for any change resulting in an Incident must be updated and resubmitted for review and approval.

Process Flow

See Standard Change Process Flow – Addendum B

Roles and Responsibilities

Responsibility Matrix: Standard Change Release					
Task	Service Owner	SOP SME	VCCG	Agencies / OTS	Assigned Technician
Draft Standard Operating Procedure	A	R		-	
Approve Standard Operating Procedure	R	C	A		
Create/submit RFC for Standard Change	C	C	A		R
Create Schedule of Changes	A	A			R
Create Change Ticket Entry	A	C			R
Issue Planned Standard Change Deployment Notification	A		I	I	R
Execute Change	A				R
Issue Post Deployment Notification	A		I	I	R
Complete Post Deployment Change Closure	A				R
Create Incident if disruption occurs	A			-	R
Conduct Post Implementation Review and Root Cause Analysis if disruption occurs	A				R
Update SOP as needed	A	R			C

Legend:

- SOP SME – Standard Operating Procedure Subject Matter Expert
- VCCG – Vertical Change Control Group
- R – Responsible
- A – Accountable
- S – Support
- C – Consult
- I – Inform

Normal Change: A Normal Change does not have a pre-approved SOP, is not classified as an Emergency Change, and can be deployed during a predefined, standard maintenance window. These changes must follow the full Change Management Process.

1. Change Request and Review

1.1. The Analyst will complete the Request For Change (RFC) Form (*See Addendum D*) and a corresponding ticket entry. This includes coordination of impact and risk analysis, test plan and coordination, and identification of affected stakeholders that must approve the RFC.

1.2. The following fields must be completed in the corresponding ticket entry:

1.2.1. The ticket entry must have the following fields populated:

1.2.1.1. Request Type

1.2.1.2. Classification

1.2.1.3. Change Scope
1.2.1.4. Subject
1.2.1.5. Description
1.2.1.6. Contact
1.2.1.7. Priority
1.2.1.8. Notification

1.2.2. The Completed Request For Change form must be attached to the ticket entry.

1.3. The completed RFC, including the corresponding ticket number, will be sent to Service Owner and appropriate pre-approvers for review, updates and approvals.

1.4. Once approved, the RFC will be submitted to the PPMO for inclusion in the next ECCG Meeting Agenda. PMO will review the RFC to determine readiness for review, priority and timing for ECCG Meeting. **(See ECCG – Change Management Approval below for review questions)**

2. ECCG Review and Approval

2.1. Each RFC will be reviewed and voted on by the ECCG

2.1.1. ECCG will review the RFC as outlined in the section below (ECCG - Change Management Approval)

2.1.2. Upon Approval, the release date / time will be confirmed and documented and a releaser assigned – *See Addendum H*

2.1.3. If not approved due to missing or erroneous information, a remediation period is available to correct any outstanding issues

3. Deployment into Production

3.1. At the start of the standard or approved change window, the assigned technical SME will communicate via the service owner approved communication plan to service subscribers/consumers notifying recipients that the change window is about to begin.

3.2. The assigned technical SME will then execute the steps as outlined in the change release notes.

3.3. Upon completion of the change implementation, the technical SME will execute the test plan as documented in the RFC.

3.3.1. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue including execution of the back out plan based on the criteria and steps outlined in the RFC.

3.4. Upon verifying successful implementation of the change, the technical SME will transition to the appropriate testers for regression and/or post implementation testing as outlined in the RFC.

4. Post Implementation Testing and Successful Deployment

4.1. If so documented in the Request For Change, the Business Unit will execute the test plan as documented in the RFC.

4.1.1. If the desired expectations are met, the technical SME will be notified.

4.1.1.1. The technical SME will update all documentation, including the change ticket and a Post Implementation Review (if required by ECCG), and communicate via the service owner approved communication plan to service subscribers/consumers

4.1.2. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue.

4.1.2.1. If issue resolution does not address the issue within the parameters outlined in the back out plan, the back out plan will be implemented as outlined in the RFC, including communication to appropriate affected resources.

4.1.3. If a Normal Change is low-risk and is likely to reoccur, the applicable governing body or Service Owner will consider whether to request the creation of a SOP to handle this type of change in the future. Once an SOP is created by technical SMEs and approved by ECCG, future changes of this type will be handled as Standard Changes.

5. Failed Deployment

5.1. If during the release, one or more of the changes results in a disruption of service or service level, an Incident must be created and the Incident Management Process must be followed.

5.2. Once resolved and the changes completed, a Post Implementation Review and Root Cause Analysis must be completed and attached to the ticket item.

Process Flow

See Normal/High Priority Change Process Flow – Addendum A

Roles and Responsibilities

Responsibility Matrix: Normal Change Release					
Task	Service Owner	PMO	ECCG	Agencies / OTS	Assigned Technician
Draft Request for Change (RFC) and ticket entry	A			-	R
Submit RFC for Approval	A, R				
Review RFC and assign to ECCG Agenda		A, R			
Present RFC to ECCG					
Approve RFC			A, R		
Issue Change Notification	A			I	R
Issue Change Window Start Notification	A			I	R
Execute Change	A				R
Issue Post Deployment Notification	A		I	I	R
Complete Post Deployment Change Closure	A				R
Create Incident if disruption occurs	A			-	R
Conduct Post Implementation Review and Root Cause Analysis if disruption occurs	A				R

Legend:

- PMO – Project Management Office
- ECCG – Enterprise Change Control Group
- R – Responsible
- A – Accountable
- S – Support
- C – Consult
- I – Inform

High Priority Change: A High Priority Change does not have a pre-approved SOP, is not classified as an Emergency Change, and requires deployment outside standard maintenance windows. These changes must follow the full Change Management Process.

1. **Change Request and Review**
   - **1.1.** The Analyst will complete the Request For Change (RFC) Form (*See Addendum D*) and a corresponding ticket entry. This includes coordination of impact and risk analysis, test plan and coordination, and identification of affected stakeholders that must approve the RFC.
   - **1.2.** The following fields must be completed in the corresponding ticket entry:
     - **1.2.1.** The ticket entry must have the following fields populated:
       - **1.2.1.1.** Request Type
       - **1.2.1.2.** Classification
       - **1.2.1.3.** Change Scope
       - **1.2.1.4.** Subject
       - **1.2.1.5.** Description
       - **1.2.1.6.** Contact
       - **1.2.1.7.** Priority
       - **1.2.1.8.** Notification
     - **1.2.2.** The Completed Request For Change form must be attached to the ticket entry.
   - **1.3.** The completed RFC, including the corresponding ticket number, will be sent to Service Owner and appropriate pre-approvers for review, updates and approvals.
   - **1.4.** Once approved, the RFC will be submitted to the PMO for inclusion in the next ECCG Meeting Agenda. PMO will review the RFC to determine readiness for review, priority and timing for ECCG Meeting. **(See ECCG – Change Management Approval below for review questions)**
2. **ECCG Review and Approval**
   - **2.1.** Each RFC will be reviewed and voted on by the ECCG
     - **2.1.1.** ECCG will review the RFC as outlined in the section below (ECCG - Change Management Approval)
     - **2.1.2.** Upon Approval, the release date / time will be confirmed and documented and a releaser assigned – *See Addendum H*
     - **2.1.3.** If not approved due to missing or erroneous information, a remediation period is available to correct any outstanding issues
3. **Deployment into Production**
   - **3.1.** At the start of the standard or approved change window, the assigned technical SME will communicate via the service owner approved communication plan to service subscribers/consumers notifying recipients that the change window is about to begin.
   - **3.2.** The assigned technical SME will then execute the steps as outlined in the change release notes.
   - **3.3.** Upon completion of the change implementation, the technical SME will execute the test plan as documented in the RFC.

3.3.1. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue including execution of the back out plan based on the criteria and steps outlined in the RFC.

3.4. Upon verifying successful implementation of the change, the technical SME will transition to the appropriate testers for regression and/or post implementation testing as outlined in the RFC.

4. Post Implementation Testing and Successful Deployment

4.1. If so documented in the Request For Change, the Business Unit will execute the test plan as documented in the RFC.

4.1.1. If the desired expectations are met, the technical SME will be notified.

4.1.1.1. The technical SME will update all documentation, including the appropriate ticket and a Post Implementation Review (if required by ECCG), and communicate via the service owner approved communication plan to service subscribers/consumers

4.1.2. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue.

4.1.2.1. If issue resolution does not address the issue within the parameters outlined in the back out plan, the back out plan will be implemented as outlined in the RFC, including communication to appropriate affected resources.

5. Failed Deployment

5.1. If during the release, one or more of the changes results in a disruption of service or service level, an Incident must be created and the Incident Management Process must be followed.

5.2. Once resolved and the changes completed, a Post Implementation Review and Root Cause Analysis must be completed and attached to the ticket item.

Process Flow

See Normal/High Priority Change Process Flow – Addendum A

Roles and Responsibilities

Responsibility Matrix: High Priority Change Release					
Task	Service Owner	PMO	ECCG	Agencies / OTS	Assigned Technician
Draft Request for Change (RFC) and ticket entry	A			-	R
Submit RFC for Approval	A, R				
Review RFC and assign to ECCG Agenda		A, R			
Present RFC to ECCG					
Approve RFC and alternate Change Window			A, R		
Issue Change Notification	A			I	R
Issue Change Window Start Notification	A			I	R
Execute Change	A				R
Issue Post Deployment Notification	A		I	I	R
Complete Post Deployment Change Closure	A				R
Create Incident if disruption occurs	A			-	R
Conduct Post Implementation Review and Root Cause Analysis if disruption occurs	A				R

Legend:

- PMO – Project Management Office
- ECCG – Enterprise Change Control Group
- R – Responsible
- A – Accountable
- S – Support
- C – Consult
- I – Inform

Emergency Change: An Emergency Change is a change that must be deployed as soon as possible in order to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs).

Release Approval

1.1. Once a resolution for the outage and/or severe service disruption has been identified, communications containing details with the issue, proposed resolution, associated ticket numbers, known impact and risk, must be sent to following the OTS Incident Management policy/plan

1.2. In addition, the Business Units will be notified that a resolution has been identified and an Emergency Change is being planned to resolve it.

1.3. The Emergency Change can be executed once a minimum of one (1) Service Owner has approved, or CIO/Deputy CIO have approved, verbally or via email.

1.4. If no verbal or written approval is received within 30 minutes, the Service Owner will provide approval to proceed.

1.5. An email to the entire organization will be sent notifying them of any outage or service disruption that will occur as a result of the Emergency Change window. This will include the service(s) affected and the potential duration of the interruption.

1.6. The assigned technical SME will execute the change as outlined in the emergency change documentation.

1.7. Upon completion of the change implementation, the technical SME will execute the test plan as documented in the emergency change documentation.

1.7.1. If the test fails, the technical SME will utilize approved troubleshooting techniques to correct the issue.

1.8. Once service is restored, a notification will be sent following the OTS Incident Management policy/plan

1.9. A separate communication will be sent to the business units notifying them of resolution and service restoration.

1.10. If written approval was not received prior to the emergency change release, retroactive acknowledgement of verbal approval, or acknowledgement that change qualified as an Emergency Change and was appropriate to deploy without approval, will be completed.

1.11. Additionally, Change ticket and related Incident tickets in the ticketing system will be updated

1.11.1. The ticket entry must have the following fields populated:

1.11.1.1. Request Type

1.11.1.2. Classification

1.11.1.3. Change Scope

1.11.1.4. Subject

1.11.1.5. Description

1.11.1.6. Contact

1.11.1.7. Priority

1.11.1.8. Notification

1.11.2. The Completed Request For Change form must be attached to the ticket entry.

2. Post Implementation Review and Root Cause Analysis

2.1. All Emergency Changes will require a Post Implementation Review and Root Cause Analysis – *See Addendum I*

Process Flow

See Emergency Change Process Flow – Addendum C

Roles and Responsibilities

Responsibility Matrix: Emergency Change Release					
Task	Service Owner	CIO / Deputy CIO	ECCG	Agencies / OTS	Assigned Technician
Draft Request for Change (RFC) and ticket entry	A			-	R
Submit RFC for Approval	A, R				
Approve Emergency Change		A, R	I		
Issue Emergency Change Notification	A			I	R
Issue Emergency Change Start Notification	A			I	R
Execute Change	A				R
Issue Post Deployment Notification	A		I	I	R
Complete Post Deployment Change Closure	A				R
Create Incident if disruption occurs	A			-	R
Conduct Post Implementation Review and Root Cause Analysis	A				R

Legend:

- ECCG – Enterprise Change Control Group
- R – Responsible
- A – Accountable
- S – Support
- C – Consult
- I – Inform

5. POST IMPLEMENTATION REVIEW

Objective: The objective of a Post Implementation Review is to assess the course of the Change implementation and the achieved results, in order to provide a complete history for a change and to make sure that any issues are analyzed and lessons learned.

In order to maximize the benefit of this process while balancing time and resource utilization, the following guidelines will be used to determine when and how a Post Implementation Review is needed:

5.1. PROCESS

1. A Post Implementation Review will be completed within the following guidelines for each change type
   1.1. Standard Change/Release: A periodic audit is to be conducted annually on Standard Changes.
      1.1.1. A sample subset of Standard Changes completed during the time window indicated above will be selected
      1.1.2. Vertical Change Managers will review the process and result of each Standard Change in the sample set and determine
         1.1.2.1. Number or times/percentage a Standard Change resulted in an Incident
         1.1.2.2. Execution and result of functional and/or operational tests
         1.1.2.3. Actual versus planned implementation start, end and duration
         1.1.2.4. Actual versus planned acceptance test start, end, duration, participants and results
         1.1.2.5. Adherence to documentation and communication requirements including close out documentation in Change Record

   1.2. Normal Change/Release and High Priority Releases: Post Implementation Reviews for Normal Change/Release and High Priority Releases will be determined as part of the Change Approval process by the Enterprise Change Control Group (ECCG) and as a result of periodic audits to be conducted annually
      1.2.1. As part of the Change Management Process, during Approval by the Change Management Approval Authority (ECCG or VCCG), a decision will be made on whether a full Post Implementation Review is required for the Change.
      1.2.2. In addition, a sample subset of Normal and High Priority Changes completed during the time window indicated above will be selected
      1.2.3. Enterprise Change Managers will review the process and result of each Normal Change/Release and High Priority Releases required to do so by the Enterprise Change Control Group (ECCG), or in the sample set, and document
         1.2.3.1. Adherence to Change requirements, procedures, tests, back out plans as outlined in the original request
         1.2.3.2. Execution and result of functional and/or operational tests
         1.2.3.3. Summary of test results
         1.2.3.4. Actual versus planned implementation start, end and duration
         1.2.3.5. Actual versus planned acceptance test start, end, duration, participants and results
         1.2.3.6. Number and percentage of Normal and High Priority Changes resulting in Incidents including a Root Cause Analysis (see below)

1.2.3.7. Adherence to documentation and communication requirements including close out documentation in Change Record

1.3. Emergency Change: Post Implementation Reviews are always required for Emergency Changes and must include a Root Cause Analysis (see below).

1.3.1. When an Emergency Change must be executed, the governing body will coordinate and review the process and result for the Emergency Change in order to evaluate and document the reason for the emergency change and potential mitigation steps

1.3.1.1. Adherence to change requirements, procedures, tests, back out plans as outlined in the original request

1.3.1.2. Execution and result of functional and/or operational tests

1.3.1.3. Summary of test results

1.3.1.4. Actual versus planned implementation start, end and duration

1.3.1.5. Actual versus planned acceptance test start, end, duration, participants and results

1.3.1.6. Any additional resulting Incidents including additional Root Cause Analysis (see below)

1.3.1.7. Adherence to documentation and communication requirements including Emergency categorization and close out documentation in Change Record

2. A Post Implementation Review and Root Cause Analysis will be required, regardless of Change Type, any time that a change results in an Incident, outage, service interruption, or results/process of change are not as expected/documented.

2.1. In these cases, a Root Cause Analysis will also be required as part of the Post Implementation Review

2.2. The EUC Incident Manager will review the process and result of the Change and document

2.2.1. Adherence to Change requirements, procedures, tests, back out plans as outlined in the original request

2.2.2. Execution and result of functional and/or operational tests

2.2.3. Summary of test results

2.2.4. Actual versus planned implementation start, end and duration

2.2.5. Actual versus planned acceptance test start, end, duration, participants and results

2.2.6. Resulting Incidents including a Root Cause Analysis (see below)

2.2.7. Adherence to documentation and communication requirements including close out documentation in Change Record

3. When a Root Cause Analysis is required per the guidelines above, the following information will be included (see Addendum I for Root Cause Analysis template)

3.1. Related Change ID and Title

3.2. Incident Date

3.3. Incident Number

3.4. Service Owner(s)

3.5. Root Cause Author

3.6. Date of Root Cause Analysis

3.7. Incident Description (Including Impacted Areas and Impact Duration)

3.8. Observations

3.9. Root Cause Analysis (including resulting resolution)

3.10. Contributing Factors

3.11. Recommendations

6. KEY PERFORMANCE INDICATORS

Objective: The objective of Key Performance Indicators is to provide a comprehensive framework for process control through regular quality assessments of the Change Management process in order to evaluate if the process is running according to expectations and/or if changes to the process are required.

The KPIs and metrics listed below reflect specific and quantifiable indicators to evaluate the quality of the process and ensure ongoing optimization and process design improvements. KPIs are reported quarterly, however, Executive Staff may require more frequent reporting of metrics and KPIs as necessary.

Critical Success Factor	Definition
Zero or near zero outages introduced by normal changes	The number of outages introduced by a normal change will be negligible due to proper completion of the change process

Key Performance Indicator	Definition
No production changes implemented w/o an RFC	The number of Standard, Normal, and Emergency Changes (reported quarterly) that is approved, retroactively approved, successful, or unsuccessful without a documented RFC will not exist

Metrics	Definition
Number of Changes by Change Type	Number of Standard, Normal, High Priority and Emergency Changes completed (approved, retroactively approved, successful, or unsuccessful) with a corresponding percentage rate
Normal or High Priority Change Acceptance Rate	Number of accepted vs. rejected RFCs as a percentage of the Number of Normal and High Priority Changes
Emergency Change Acceptance Rate	Number of Emergency Changes approved as a percentage of the Total Number of Changes
Rollback Rate	Number of changes successfully executed (per plan, no rollbacks) in a time period as a percentage of the total changes in that time period
Impact Rate	Number of changes with a resulting extended outage, major or critical Incident or Problem in a time period as a percentage of the total changes in that time period
Unapproved Rate	Number of changes completed in Production where required approval (change governing body or existing SOP for Standard) was not documented prior to execution in a time period as a percentage of the total changes in that time period

7. CHANGE MANAGEMENT APPROVAL

Objective: The objective of Change Management Approval is to define and detail the distributed change management approach of using the ECCG (Enterprise Change Control Group), to ensure that OTS is prepared to implement and support Enterprise Changes being requested, and provide oversight to the VCCG (Vertical Change Control Groups) as local or vertical changes are implemented.

7.1. ENTERPRISE CHANGE CONTROL GROUP (ECCG)

The ECCG is comprised of the following members. This group is charged with overseeing the Change Management process for the enterprise as a whole, executing the normal, high priority, and emergency change management processes for enterprise level changes, coordinating the impact analysis for enterprise change requests and making final decisions on enterprise change deployment schedules.

Members:

Topic	Enterprise Change Control Group
Chair	OTS Portfolio Dep. Director
Co-Chair	Governance Architect
Members	CTO
	PPMO Director
	CSO
	CDO
	OTS PSS Director
	OTS App Dev Director
	OTS DCO Director
	OTS EUC Director
Invited Participants	OTS Compliance Manager(s)
	Any Operational Manager
	Any Impacted Business Member
	Any Enterprise Architect
	Any Agency Relationship Manager (ARM)
Voting Method	Unanimous w/Escalation
Meeting Cadence	Monthly

Note: A minimum Quorum of 50% voting members must be present to conduct the meeting. However, voting method is unanimous for ALL voting members

7.2. VERTICAL CHANGE CONTROL GROUP (VCCG)

The VCCG is comprised of the following members. This group is charged with executing the standard, normal, high priority, and emergency change management processes for local or vertical level changes, coordinating the impact analysis for local or vertical level change requests and making final decisions on local or vertical change deployment schedules.

Members:

Topic	Vertical Change Control Group
Chair	OTS Operational Director(s)
Co-Chair	Vertical Compliance Manager(s)
Members	OTS Operational Manager(s)
	InfoSec
	Others as approved by the EGG
Invited Participants	EUC (consulted)
	Any Enterprise Architect
	Any Impacted Business Member
	Any Agency Relationship Manager (ARM)
Voting Method	Unanimous w/Escalation
Meeting Cadence	Weekly

Note: A minimum Quorum of 50% voting members must be present to conduct the meeting. However, voting method is unanimous for ALL voting members

1. **Enterprise Change Control Group Review and Approval**
   - **1.1.** All enterprise level Requests for Change (RFCs) will be previewed by the Enterprise Governance Architect and evaluated against the following:
     - **1.1.1.** Is all the required information in the RFC completed?
     - **1.1.2.** Is the timing and duration of the change documented and understood?
     - **1.1.3.** Is all the required documentation available?
     - **1.1.4.** Is the priority and impact of the change understood and documented?

1.1.5. Is each operational unit and business unit affected aware of and prepared for the change?

1.1.5.1. Is the ARM and BU contact aware and prepared for the change, including available in the event of an issue or question?

1.1.5.2. Does the change identify the owner of the Regression/Post Implementation Plan and is he/she aware and available?

1.1.6. Is the Back-Out strategy adequate for the type of change?

1.1.7. Is the change type assigned correctly?

1.1.8. Will a Post Implementation Review be required for the change?

1.2. Once reviewed for readiness and priority, the PMO will assign the change to an ECCG Meeting Agenda.

1.3. The appropriate Compliance Manager will present all Requests For Change (RFCs) for review at the ECCG meeting assigned to the RFC.

1.4. ECCG will review each RFC and validate the PMO's evaluation of the readiness and priority as determined during 1.1 above.

1.5. ECCG will provide Approval confirming the following:

1.5.1. The date and time of the change.

1.5.2. The individual performing the change.

1.6. The Service Owner that owns the systems under the change will certify the information and notify the organization of the pending changes following their communication plan.

2. Standard Changes and Standard Operating Procedures

2.1. Prior to a change being categorized as Standard, Vertical Change Control Group (VCCG) must review and approve as follows:

2.1.1. A Standard Operating Procedure must be documented and presented for review along with the request to categorize a repeatable change as Standard.

2.1.2. VCCG will review the request and SOP and evaluate against the following:

2.1.2.1. Is the change repeatable and predictable?

2.1.2.2. Is the change low-risk with limited to no impact on OTS Services?

2.1.2.3. Is the Standard Operating Procedure thorough and does it address all the needed steps and information for clear execution?

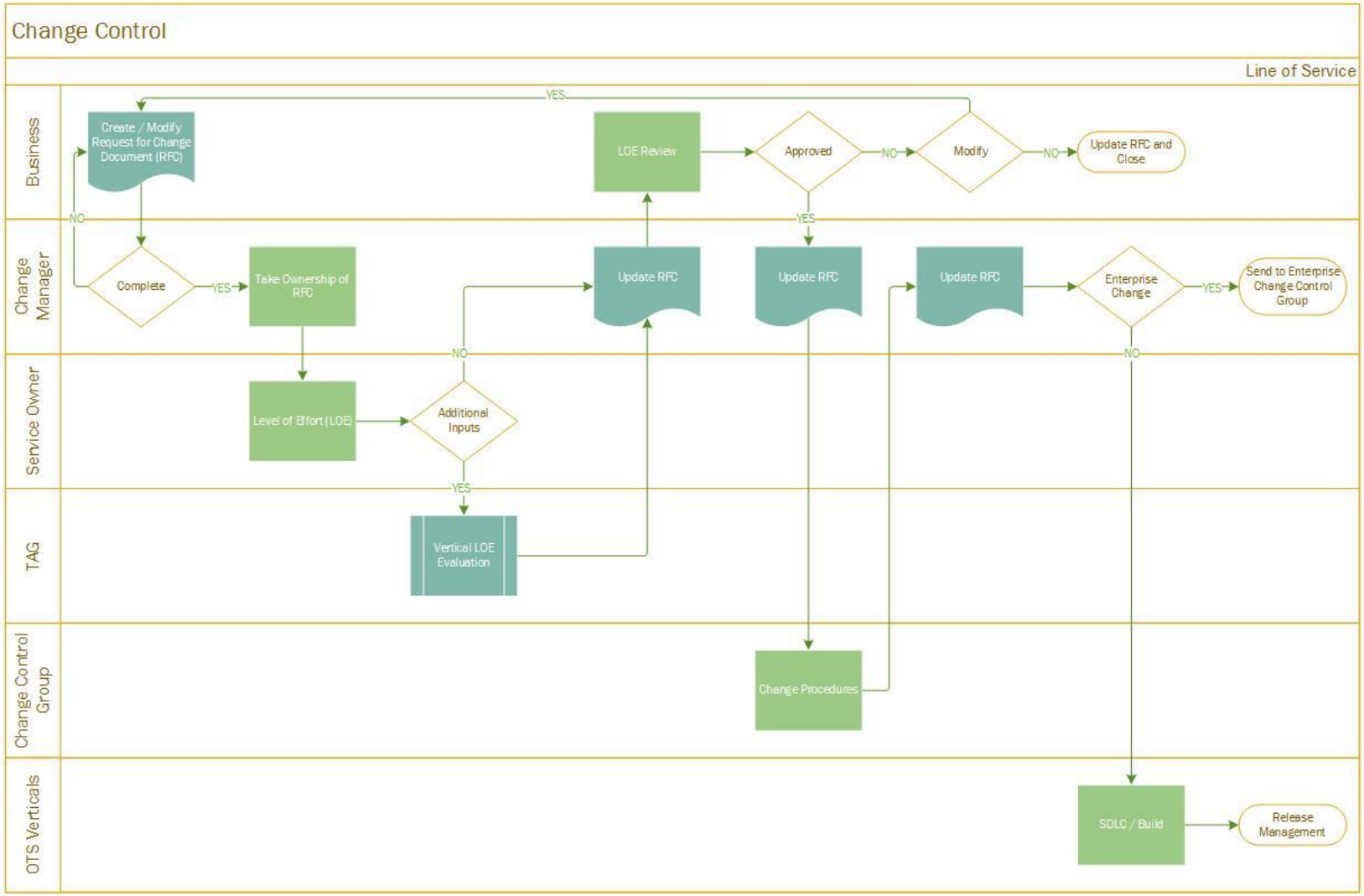
2.1.2.4. Has the change been conducted in the past with repeatable results and limited to no resulting incidents?

2.2. Vertical Change Control Group (VCCG) will approve the request and SOP, certifying the information via meeting minutes

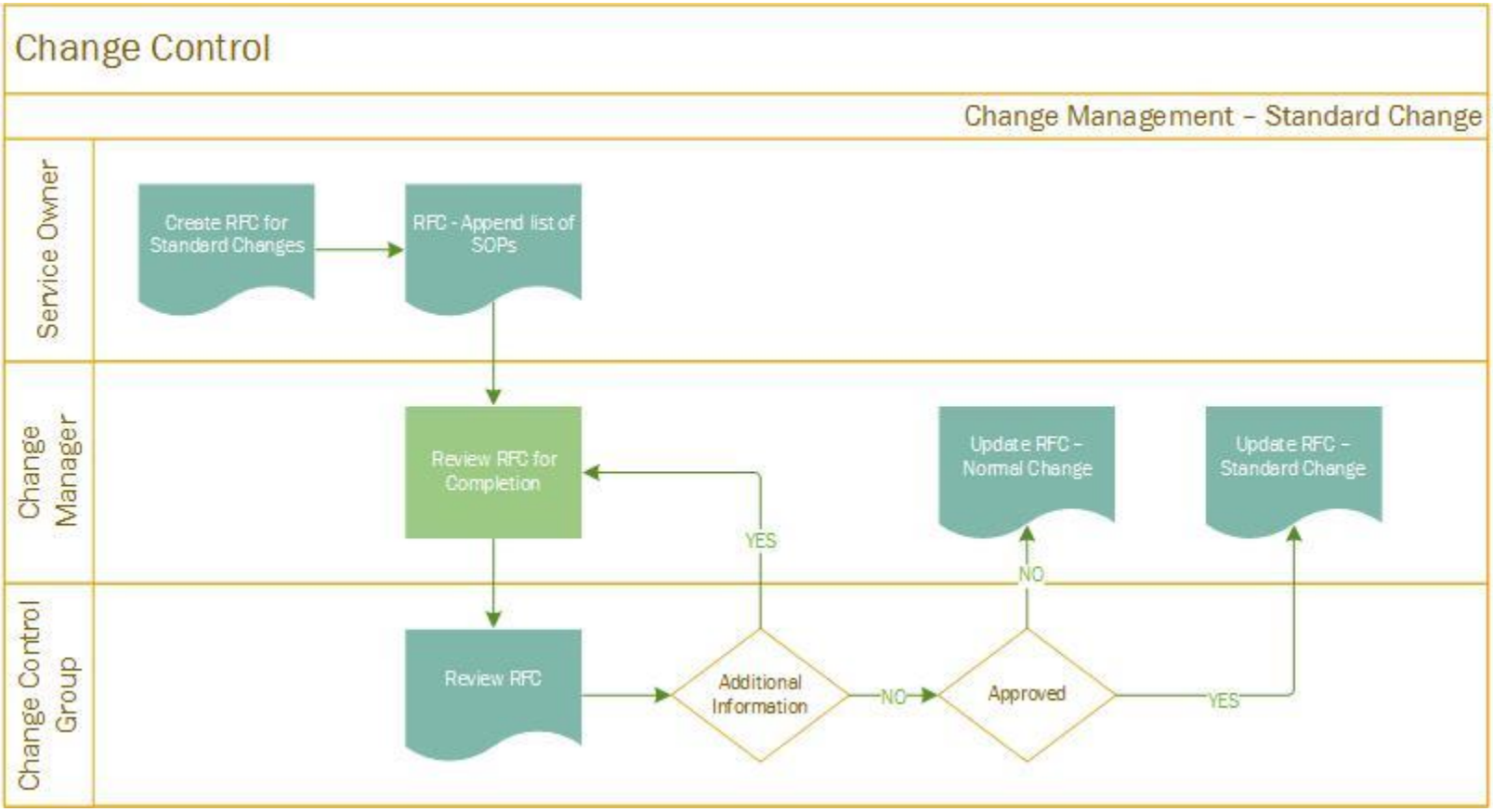
7.3. EMERGENCY CHANGE MANAGEMENT APPROVAL

Emergency Changes will be handled as noted above in Emergency Change Processes. Notification will be sent to ECCG and approval from one Service Owner will be required to execute the change. CIO and/or Deputy CIO can provide single approval for any change.

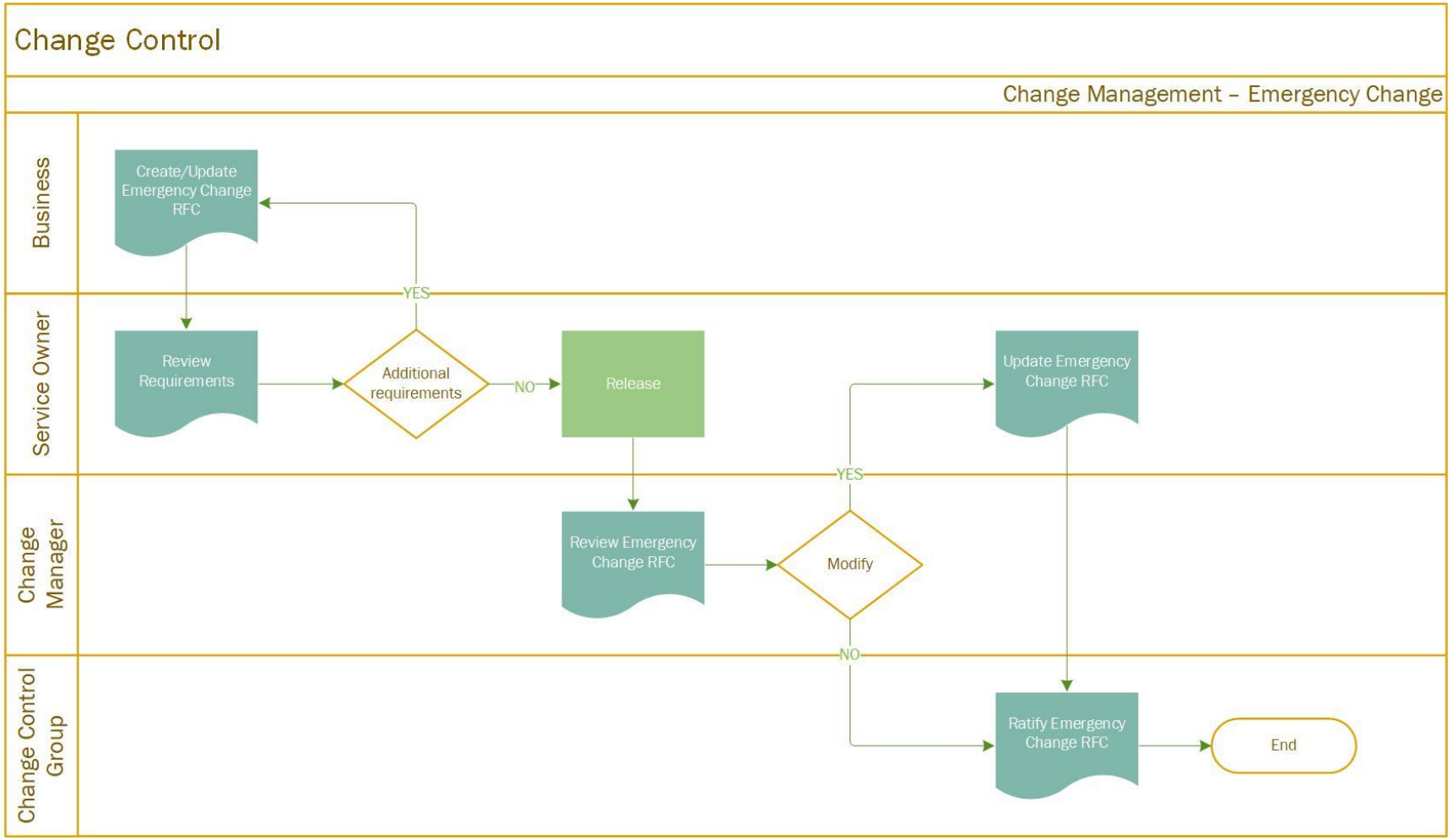
8. Addendum A – NORMAL/HIGH PRIORITY CHANGE MANAGEMENT PROCESS



9. Addendum B – STANDARD CHANGE MANAGEMENT PROCESS



10. Addendum C – EMERGENCY CHANGE MANAGEMENT PROCESS



11. Addendum D – REQUEST FOR CHANGE (RFC)

The RFC template is below:

Request for Change Template-v6

REQUEST FOR CHANGE INSTRUCTIONS:

1. **RFC ID:** Unique identifier for each Request For Change (RFC). The RFC ID will be the ticketing system ticket #.
2. **RFC Title:** Short, descriptive title for the change including the key System or Configuration Item affected, and a short description of the change type (e.g. Windows Servers: Security Patch xx.xxxx).
3. **Date of Submission:** Date RFC was completed and submitted for review.
4. **Date Required:** Requested target date to implement the change.
5. **Submitter Name & Title:** Name and Title of Subject Matter Expert (SME) completing the RFC form.
6. **Service Owner Name and Title:** Name and Title of Service Owner responsible for key system, or configuration item, affected by the proposed change.
7. **ARM Name & Title:** Name and Title of ARM responsible for key system, or configuration item, affected by the proposed change.
8. **BUO Name & Title:** Name and Title of Business Unit Owner (BUO) responsible for key system, or configuration item, affected by the proposed change.
9. **Related Change Proposal:** List of numbers and/or titles of all Work Orders, Incidents, Service Requests or Projects that initiated, or are dependent on, the proposed change.
10. **Change Classification:** Based on the following definitions, indicates the type of change being requested:

    a. Standard Change –a pre-authorized change that is low-risk, predictable in its outcome, and repeatable through defined work instructions in a standard operating procedure (SOP).
    b. Normal Change –a change that does not have a pre-approved SOP, is not classified as an Emergency Change, and can be implemented during predefined and standard maintenance windows. In general, all Service Requests, inputs from Project, Release and Deployment Management, and resolutions for low to high priority incidents in Incident and Problem Management, are handled as Normal changes.
    c. High Priority Change – a change that does not have a pre-approved SOP, is not classified as an emergency, and requires implementation outside of standard maintenance windows but not during operating hours such as an Emergency Change.
    d. Emergency Change –a change that must be deployed as soon as possible to resolve an outage, address severe impact to the business and/or severe impact to the security baseline, and meet operational level agreements (OLAs.)
11. **Proposed Priority:** Based on the following definitions, indicates the proposed priority of change being requested:
    a. **High:** Primary Service or Application, or Entire Enterprise, can be affected if change is not implemented; existing workarounds are not sufficient to maintain service availability, or perform required business functions.

b. **Medium**: Multiple services, or agencies, can be affected if the change is not implemented; existing workarounds are sufficient to maintain service availability, or perform required functions, but are complex and time consuming.
c. **Low:** Single service, or agency, can be affected if the change is not implemented; existing workaround are sufficient to maintain service availability, or perform required business functions.

12. Request for Change Details:

a. **System or Configuration Item to be Changed:** List of key system, or configuration item, to be changed; if multiple systems or CIs are being changed directly, please list them here.
b. **Description of Requested Change:** Brief description of the proposed change.
c. **Reason for Change:** Description of root cause and/or need for the change (e.g. Security risk resolution, outage resolution, added functionality due to existing project.)
d. **Details of Change:** Detailed information of how the change will be deployed, tested, and rolled back, if necessary, as well as resources needed for these tasks. Details must be provided as appropriate for the level of change. Attachments may be used in lieu of the comments if documentation already exists, and/or amount of information requires more space. In that case, comments should reflect link, or information to reference attachments.
    i. **Deployment Steps and Resources Required:** List of steps to be taken in deploying the proposed change. Steps should be listed in the order in which they will occur, as well as expected results, or additional commands, to be entered at resulting prompts/steps. Resources for each subset of steps should be listed. This section should also include details of the communication plan, including resources/method/timing, to issue notifications for testing to begin, and/or issue escalation; include resources/method/timing for start, and end of change notifications, if different than Standard Change management processes. For Standard Changes, a reference to all applicable SOPs is sufficient.
    ii. **Regression / Post Implementation Test Plan and Resources Required:** List of specific tests that will be conducted once the change has been deployed, as well as resources needed to conduct each test. Outline testing to be completed by Technical SMEs, as well as by Business Units/Resources, if appropriate. For Standard Changes, a reference to all applicable SOPs is sufficient.
    iii. **Remediation/Back Out Plan:** Outlines the known steps to be taken to remediate any issues with the change deployment, as well as the criteria to be met to trigger rollback of the changes, versus continued issue resolution. Also includes the procedures and plans to back out the deployed change(s). For Standard Changes, a reference to all applicable SOPs is sufficient.
e. **Business Impacts:** Detailed information of impact to the business per specific categories below. Attachments may be used in lieu of the comments if documentation already exists, and/or amount of information requires more space. In that case, comments should reflect link, or information to reference attachments.

i. **Other Services, Applications, Agencies, Customers Affected by this change:** List of systems, services, applications, agencies, or customers that will be affected by the requested change, as well as details of the impact (e.g. outage, change in functionality).

ii. **Expected Outage Duration:** Indicates the expected duration of outage to deploy the change, as well as any other outages that occur as a result of the change, but have a different duration or time window.

f. **Risk of Change & Mitigation Plan:** Description of risk associated with implementing the change, and any mitigation plans in place, or to be executed, to minimize the risk.

g. **Risk of Not Implementing Change:** Description of risk if the change is not implemented.

13. Approved By:

a. **Service Owner Name & Title:** Name and Title of Service Owner that approved the RFC.

b. **Approval Method & Date:** Method of approval (verbal, email, hard copy signature) and the date received.

c. **ARM Name & Title:** Name and Title of ARM that approved the RFC.

d. **Approval Method & Date:** Method of approval (verbal, email, hard copy signature) and the date received.

e. **BUO Name & Title:** Name and Title of BUO that approved the RFC, if required.

f. **Approval Method & Date:** Method of approval (verbal, email, hard copy signature) and the date received.

g. **Security Reviewer Name & Title:** Name and Title of Security Team member that approved the RFC.

h. **Approval Method & Date:** Method of approval (verbal, email, hard copy signature) and the date received.

14. Approval Authority Determination

a. **Decision:** Indicates if ECCG approved the RFC, Approved with Conditions, Rejected, or Requested Further Updates prior to approving. Details for Approval Conditions or Requested Updates are to be found in the ECCG Meeting Minutes.

b. **Post Implementation Review Required:** For a Normal Change, indicates if a Post Implementation Review is required. PIR is always required for Emergency Changes, and is done on an audit basis for Standard Changes.

c. **Decision Date:** Indicates the ECCG Meeting Date where the RFC was reviewed and approved; detailed notes on the review and approval are to be found in the ECCG Meeting Notes corresponding to the date provided. If approval from ECCG, or subset of ECCG for Emergency Changes, was not received during a formal meeting, this date refers to date verbal, or email approval was received

12. Addendum E: OTS STANDARD OPERATING PROCEDURE (SOP) TEMPLATE

13. Addendum F: OTS SCHEDULE OF CHANGES TEMPLATE

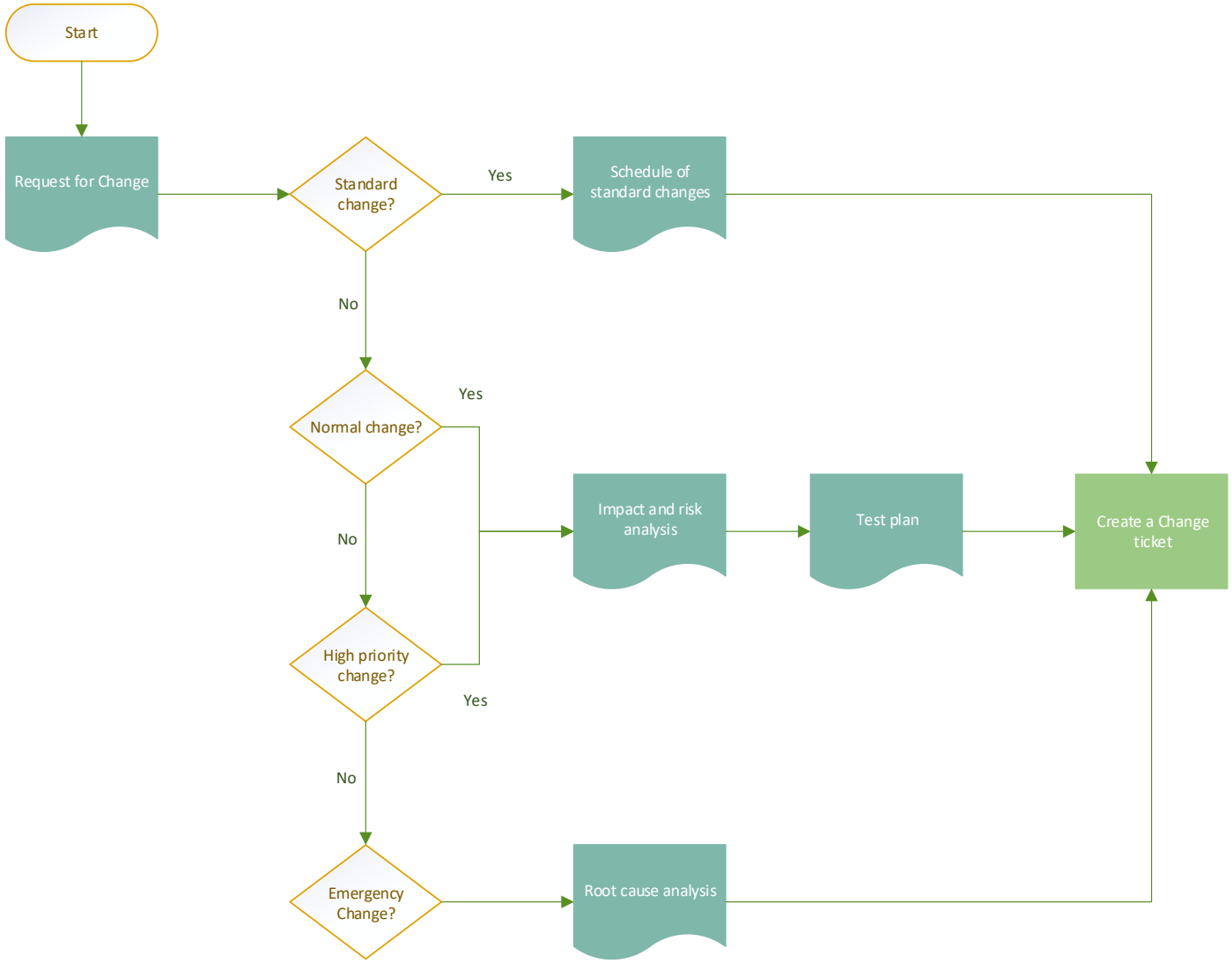
14. Addendum H – CHANGE CONTROL GROUP MEETING MINUTES EXAMPLE

Change Control Group Meeting Minutes

ECCG/VCCG Date:_____

Voting Member Present:

RFC ID #	Approval	Releaser	Date	Notes
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			
	☐ Approved ☐ Rejected			

15. Addendum I – ROOT CAUSE TEMPLATE

16. Addendum J – RFC SUBMISSION PROCEDURE DIAGRAM