Change Management Process

MaxxLogix SaaS Software Solutions

IT Operations Process Description

MaxxLogix

Table of Contents

1. Introduction

1.1 Purpose of Document

This document describes MaxxLogix LLC's Change Management Process for the software solutions they design and develop. The process is designed to allow clients or internal users to request, manage, approve and control changes that modify the software solutions we develop.

1.2 Audience

The document is intended to provide an end-end overview of the change management process and is to be used as a reference for all MaxxLogix SaaS clients.

1.3 Overview

The purpose of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes associated with a client's MaxxLogix SaaS application or applications, to minimize the number and impact of any related incidents. Changes in the IT infrastructure may arise reactively in response to problems, or proactively from seeking improved efficiency and effectiveness, as well as to enable or reflect business initiatives, programs, projects, or service improvements.

Change Management can ensure standardized methods, processes, and procedures facilitate efficient and prompt handling of all changes and maintain the proper balance between the need for change and the potential detrimental impact of changes, thus contributing to maintaining service level objectives.

This document defines the process for implementation of changes that affect managed cloud services provided by MaxxLogix LLC to its clients. Change Management does not apply to regular MaxxLogix SaaS system configuration requests from clients like adding or removing users, creating folders, searches and index forms, setting up remote scanning or updating user rights and privileges -Filtered Changes. Change Management does apply for any major hardware infrastructure, integration, workflow or online form changes. Any major application design change or new application would undergo the Change Management process.

Each step in the process is important unto itself as well as being a necessary part of the entire process. It provides a vehicle for communications, evaluation, approval, implementation, and measuring effectiveness of all changes.

The Change Management Process begins with the identification, recording, and classification of the change, and continues with its approval, test, and staging for implementation. Once the completed implementation has been measured and reported, the Change Process is complete.

2 Objective

The objectives of this process are as follows:

- Provide a structured process for planning, scheduling and implementing changes.
  - Measured by number of changes.
    - Performed within the scope of the approval process.
    - Tested successfully.
    - Implemented successfully.
- Minimize downtime.
  - Measured by downtime resulting from unapproved, unscheduled or unsuccessful changes.

3 Process Triggers

Any MaxxLogix SaaS application changes that fall outside what is deemed to be regular application support or maintenance would be considered as a change process trigger.

4 Key Terms and Definitions

Term	Definition
Action Items	The purpose of the Action Items is to provide detailed change implementation steps. Action Items are not a replacement for project plans, design reviews, or other planning activities. Action Items should be utilized to indicate the activities group(s) or individual(s) that are responsible for completing the requested change. They also provide a historical record for future reference and lessoned learned.
Approver	A member of the Approval Groups for the platform or service being changed or affected. Responsible for assuring the total quality of all requests including all documentation requirements. Has the authority to approve or reject changes.
Approver Group	Group of individuals authorized and responsible for the review and approval of Change Requests.

Back Out Plan	A contingency plan of step-by-step instructions with defined success criteria (with sufficient detail to allow an individual with similar skills to execute the plan and is understood by all approvers) to minimize any disruption of service if a change implementation does not go as planned.
Change Management	The process used to ensure that any modifications to the MaxxLogix SaaS environment are performed in a controlled and approved manner.
Configuration Item (CI)	Configuration Item or CI refers to the fundamental structural unit of a configuration management system. Examples of CIs include documents, hardware, software, models, plans, and people.
Implementation	The enactment of a change to a platform service or facility
Implementation Plan	A step-by-step set of instructions detailing information on how the proposed change will be implemented and tested. Level of detail must be sufficient for a person with similar skill to execute the implementation successfully and be understood by all reviewers/approvers.
Implementer	The person/assignee or group of individuals who perform implementation of a change activity. If the Implementer does not have Change Management system access, it is the responsibility of change owner to close the Change Request with success/failure detail.
Lead Time	The required amount of time between when a Change Request is submitted and the change. start date/time.
Post Implementation Review (PIR)	Review of changes from the prior change period. Should include noting any problems/resolutions with changes performed during that period.
Request for Change (RFC)	Tickets submitted to request a change to MaxxLogix SaaS or MaxxLogix Enterprise software. Also known as a Change Request.
Requester/ Owner	The person responsible for documenting, planning, coordinating, implementing (or assigning an implementer) and closing a Request for Change This person inputs the Change Request into toolset.
Risk Assessment Matrix	A matrix of the level of risk for each aspect of a change – scope, impact, complexity, severity, users and location.

Service Desk	A tool implemented at MaxxLogix LLC to facilitate service management. The current implementation is a repository for all service desk interactions, incidents (both from callers and alerts), service desk knowledge, and on-call support contacts.
Standard Change Request (SCR)	A document that describes the requested change and why it is important. This can originate from problem reports, system enhancements, other projects, changes in underlying systems, and senior management.
Technical Change Approver	The person responsible for the change process for a client department or group, typically within the requester's organization.

5 Change Management Process Flow

Change Management includes the following sub-processes:

- Change Request by Customer or MaxxLogix LLC Notifies Customers of an Upcoming Change
- Change Review
- Change Assessment and Planning
- Change Approval Customer Form
- Coordinate Change Implementation
- Change Testing Validation and Closure

6 Change Management Processes – End-to-End

6.1 Submit/Re-Submit Change Request

The person or group responsible for requesting the implementation of a change has the responsibility of documenting and submitting the Change Request.

Prior to preparation of a Change Request, all technical aspects of a change should be coordinated between the Requester and the personnel whose responsibility it will be to implement the change. Changes should be tested prior to implementation and information regarding the success/failure of tests included in the Change Request.

Once the Change Request Start Date/Time has passed, if a scheduled change is not to be implemented the change must be cancelled. If the change is attempted at a later date/time, a new request must be opened with the new implementation date/time and approvals obtained.

6.1.1 Defined Scope

Defining the scope of a change includes identifying the platforms impacted, duration of any outage requirements, business units or departments affected and an assessment of risk. This data is used in many decision points within the process.

The complexity of changes must be understood and communicated to change Approvers. Appendix A contains a list of Change Request details that should be considered when drafting a Change Request. Any additional information that is vital to understanding a change must be included when defining a change.

6.1.2 Draft Change Request

Once the scope of a change is defined, the data should be drafted into a Change Request as soon as it is available. Drafting a Change Request as soon as information becomes available allows data to be reviewed at an early stage.

All details pertaining to implementation, testing and backup plans must be documented within the change record itself. Attachments are permissible for supporting documentation only. (i.e., test scripts, project plans, etc.).

In addition to providing details of the change, it is the responsibility of the Requester to identify the level of risk associated with the change. The Risk Assessment in Appendix B must be used to identify risk of all changes.

Change Categories

There are three main designated categories of Change Requests (Normal, Filtered, and Emergency). These categories are based on both the Risk Level Assessment (RLA) and time between submission of a Change Request, and the Start Date of the change. Change Categories are reviewed in PIR and reported in Change Management metrics.

Normal Changes are defined as changes that meet required lead-time, submission cut-off time, and maintenance window (if applicable). Normal Changes must follow all Change Management Procedure activities unless they are defined and approved as Filtered Changes.

Filtered Changes are a pre-defined subset of Normal changes that have been identified as having no impact, or outside the scope of the Change Management process. Filtered Changes require the submission of an email from the client for tracking and recordkeeping purposes but will not have an associated approval process.

Emergency Changes are defined as changes required to immediately restore service or to avoid an outage where no other workaround is available. Upon approval, a Change Request may be entered after change implementation.

6.1.3 Submit Request

Changes must be submitted with the appropriate lead time to ensure that appropriate individuals receive adequate notice of changes.

6.2 Review Change Request

Once a Change Request is submitted, a review process begins. There is a minimum of two levels of review prior to Change Requests being scheduled (approved for implementation. This section describes the activities performed during leading to approval by the Technical Change Approver.

6.2.1 Verify Change Specifications

Each Approver Group must have predetermined individuals (primary and backup) responsible for reviewing all Change Requests that have specified their group as Approvers (either as an Approver or a group to notify). This resource is responsible for reviewing all changes affecting their group that are planned for implementation. The resource will assess the impact on their group and notify all members of his/her workgroup. If the information in the Change Request is sufficient to warrant approval, the group approves the request. If the information is not sufficient, follow the guidelines in the Review for Issues / Conflict section below.

In addition to the Information to include in Change Requests in Appendix A, the following should be considered during the evaluation of every change request submission:

- Date/time/duration of the change.
- Description of the change
- Risk assessment
- Technical validity of activities
- Justification for change
- Impact to schools/business units and to other scheduled changes
- Teams identified on Approver and Notification lists.
- Potential conflicts – Owners of conflicting changes to resolve conflicts/escalate to management.
- Detailed Test Plan – including detail of testing success/failure.
- Detailed Implementation Plan
- Detailed Back out Plan - – including detail of testing success/failure.
- Disaster Recovery impact
- Go/No-Go point (if necessary)
- Security Impact assessment – if security impacted, testing & approval from Security required

Review for Issues / Conflicts

If an Approver has concerns or questions about a change and the information provided is not sufficient, the Approver may either request further information be added to the record, request the Change Request be rescheduled, or reject the change. Approvers must document any reason for rejection within the change record.

6.2.2 Allocate Required Resources

For any change to be successful, appropriate resources must be allocated to the implementation of that change. The following are examples of resources to consider for all changes:

- Time within a scheduled change window
- Personnel to implement and support the change.
- Logical and physical access
- Interfaces with other groups to ensure adequate testing facilities.
- Interface with customers to negotiate and agree on service outages, degradation of service(s) or additional requirements.

6.2.3 Approve or Reject Change

After review of a Change Request, Approvers may either approve or reject the request. Approvers should contact change Requesters directly as soon as possible to resolve issues. If issues cannot be resolved, the Requester may cancel or re-plan the work involved to address the issues or Approvers may reject the Change Request. It is recommended that Approvers make every attempt to resolve issues or conflicts prior to rejecting a change. Once a change is rejected, it must revert to the beginning of the process for re-approval or be cancelled.

6.3 Coordinate Change

The lead MaxxLogix Engineer is responsible for scheduling all changes (providing the final approval) and refining the final Change Schedule related to all activities being performed.

6.4 Implement Changes

All changes require appropriate levels of approval prior to the planned start date and time.

The Implementer, normally the Change Requester, performs the implementation of the change. It is the responsibility of the Implementer to verify system availability prior to implementing the change. If the implementation is not to be performed by the Requester, the Requester designates an assignee, who may be a vendor. In cases where the assignee will not have access to the Change Management tool, it is the responsibility of the Requester to update the Change Request with implementation results.

6.5 Implement Change

The Implementer(s) should follow the implementation action items detailed in the Change Request. Any deviation from the approved implementation plan, including requirements to extend the approved change window, must be approved by a Technical Manager (who will verify appropriate approvals are obtained prior to providing final approval for deviation).

6.6 Verify Change Success

The Implementer must determine the success of the change based on execution of the post implementation test plan and success criteria identified in the Change Request. If the change was not completed successfully as planned or is incomplete, the Implementer must determine if the change should be backed out. Technical Managers, Business Managers or anyone negatively impacted by the implementation of a change may request to have a change backed out.

The criteria for a successful change:

- The change was implemented in accordance with the implementation plan.
- The change was implemented within the planned implementation timeframe.
- The change did not have unplanned customer impact.
- The change met anticipated objectives defined in the Change Request
- The change did not result in a system/application outage due to the execution of the back out plan.

6.6.1 Back Out Change

If a change fails during implementation, or cannot be completed within the approved implementation period, it must be either backed out within the approved change window or a window extension may be requested.

Backout plans should include:

- A detailed step-by-step procedure for reversing the change.
- Period needed to perform the backout.
- Backout risk.
- A plan to mitigate the severity of any potential negative impact resulting from implementation reversal.
- Detailed testing plans

If a change was not completed and backed out, all parties impacted by the unsuccessful completion of the change must be notified.

6.6.2 Report Completion Data

The Implementer is responsible for reporting the final status of the Change Request within 24 hours of implementing the change:

- Actual start and end time
- Change implementation results.
- If change was not completed successfully, additional detail:
- Failure description
- Incident # (if applicable)

6.7 Measure Change Results

Measuring change results involves a review of Change Request documentation, final implementation statuses and metrics. This review is used to refine criteria used for authorizing changes, ensure consistent application of the process, and to make refinements to the process itself.

Appendix A – Information to Include in Change Requests

This Appendix supplements the detailed information to be included in the RFC Checklist.

Who?

- Implementer
- Who will be impacted by/during implementation?
- Requester name, department, email and contact number.
- Support staff requirements.
- Escalation contact names, phone number, and beeper number.
- Additional appropriate notifications

What?

- Change type.
- Technology service or facility being changed.
- Dependencies and requirements
- Platforms needed exclusively during implementation.
- Platforms affected by/during implementation.

Why?

- Business and technical justification (i.e., problem resolution, project, benefits gained)

When?

- Proposed implementation date/time (window)
- Backout time requirements
- Expected service outage window (if applicable)
- How easily can this request be rescheduled (immovability)

Where?

- Locations affected by/during implementation.

How?

- Detailed implementation plan
- Detailed back out/ plan.
- Detailed Action Items

Risk and Impact

- Business and service impact
- Technology/business risk

Acceptance Criteria for successful implementation

Go/No-Go points must be set up for the following criteria:

  - If the implementation time requires more than 50% of the change window
  - If the backout requires more than 1/3 of the change window
  - If the backout affects the entire system (e.g., IPL or server reboot)

Additional Information

- Documentation or records needing revision.
- Problem Management record number where relevant
- Security impact detail
- Disaster Recovery impact detail
- Is this change being made to a platform or system which has DR support? If so, will corresponding changes need to be made to those systems?
- Does this result in a hardware or software configuration change?
- Does this result in a capacity change?
- Does this add additional/new business requirements?
- Updated network diagrams.
- Customer Notification/Approval

Appendix B – Risk Level Assessment

This section details how the Risk Level Assessment (RLA) is calculated.

The table below has the Risk Level Assessment weights:

Weight				
Type	1	2	3	4
Dependencies	Change cannot be backed out –or- Validation is based on usage	Complex implementation and/or validation – or- Requires extended change window –or- Change exceeds 1.5 hours to implement	Moderate implementation and/or validation	Easily confirmed and backed out
Impact	Affects All Platforms/Servers –or- Affects all sites	Exclusive use of entire platform or network –or- Affects multiple platforms/networks –or- Affects multiple systems or Business/Departments	Affects single Platform or Server –or- Exclusive use of major component – or- Exclusive use of major sub-system	System usable by users during implementation
Priority	Service outage causing for major systems	Service outage-critical component	Service outage-non Critical component	No service outage
Users Affected	75% or more users affected	50% to 75% of users affected	25% to 50% of users affected	Less than 25% of users affected
	High Risk			Low Risk

RLA	Risk
4 – 8	High
9 – 12	Medium
13 – 16	Low

Appendix C – Change Management Metrics

The following are standard Change Management metrics for hosted MaxxLogix SaaS clients:

- Minimum notice for outages (by Scheduling category)
- Sufficient test, implementation, and back out plans for all changes
- Effectiveness of change against original objectives (successful/failed)
- Trend and audit reports

The table below outlines how metrics shall be calculated in audit reports:

Metric	Calculation
% Closed Successful	# of changes "Closed Successful"/ total number of changes
% Closed Failed	# of changes "Closed Failed"/ total number of changes
% Not Closed	# of changes that are in the following status: ("Submitted," "Reviewed," “Provisional,” “Pending,” "Resubmitted," and "Scheduled")/ total number of changes
% Rejected	# of changes that are in the following status: ("Rejected")/ total number of changes
% of Cancelled	# of changes that are in ("Cancelled" and “Draft”)/ total number of changes
# of Emergency	Total # of Emergency changes
# of Normal	Total # of Normal changes
Total # of Changes	Shows the total number of Change Requests
% of Emergency	# of Emergency changes/total number of changes
% of Normal	# of Normal changes/total number of changes