



Update/Fix Testing Strategy

Last Revised:

1/24/2008

REVISION CONTROL

Document Title: CSU-CI Update-Fix Testing Strategy
Author: Joseph Dobzynski, Jr. – Department of Information Technology
File Reference: CSU-CI Update-Fix Testing Strategy.doc

Date	By	Action	Pages
8/9/2007	Joseph Dobzynski	New Document Created	All
8/15/2007	Joseph Dobzynski	Finished Draft Documentation	All
9/4/2007	Joseph Dobzynski	Updated with Neal's Comments	All
9/6/2007	Joseph Dobzynski	Updated with Neal and Angela's Comments	All
10/2/2007	Joseph Dobzynski	Updated with Neal and Nasser's Comments	All
10/11/2007	Joseph Dobzynski	Updated with Lacey Comments	All
10/18/2007	Joseph Dobzynski	Updated with Neal, Angela, Frank Comments	All
11/7/2007	Joseph Dobzynski	Updated with ASG Comments	All
1/9/2008	Joseph Dobzynski	Updated with Various Comments	All
1/24/2008	Joseph Dobzynski	Finalized with comments from Marysia, Angela	All

Review/Approval History

Date	By	Action	Pages

Table of Contents

	Page
1.0 Purpose.....	4
2.0 Roles and Responsibilities	4
3.0 Communications.....	4
4.0 Process Diagram.....	5
5.0 Process Calendar	6
6.0 Phase 1 – Planning & Analysis.....	7
6.1 Process Overview.....	7
6.2 Review Update/Fix.....	7
6.3 Analyze Update/Fix.....	7
6.4 File Update/Fix and Security Tickets.....	8
6.5 Add Update/Fix to Migration Calendar	9
6.6 Deliverables/Milestones	9
7.0 Phase 2 – Installation & Testing.....	10
7.1 Process Overview.....	10
7.2 Install Update/Fix into HCITRS	10
7.3 Test Update/Fix.....	10
7.4 Accommodate Issues	11
7.5 Deliverables/Milestones	11
8.0 Phase 3 – Implementation.....	12
8.1 Process Overview.....	12
8.2 Schedule Updates/Fixes / Security Blackout	12
8.3 Implement Updates/Fixes.....	12
8.4 Implement Security	13
8.5 Follow-Up with Module Lead	13
8.6 Deliverables/Milestones	13
Appendix A – Known Scheduling Exceptions.....	14

1.0 Purpose

The CSU-CI Update-Fix Testing Strategy supports and coordinates all testing for updates/fixes released for our Finance, Human Capital Management, and Campus Solutions systems. This strategy encompasses planning, analysis & installation, testing, and implementation to ensure each update/fix is fully tested and ready for release.

2.0 Roles and Responsibilities

Module Lead – The module lead is responsible for analyzing each update/fix, overseeing functional testing, and approving security for each update/fix.

Functional Analyst – The functional analyst is responsible for analyzing each update/fix, supporting functional testing, and providing security requirements for each update/fix. The functional analyst may be a member of ITS or a member of the department.

Technical Analyst – The technical analyst is responsible for installing each update/fix, scheduling implementation into our production environment, and ensuring all security is in place after implementation.

3.0 Communications

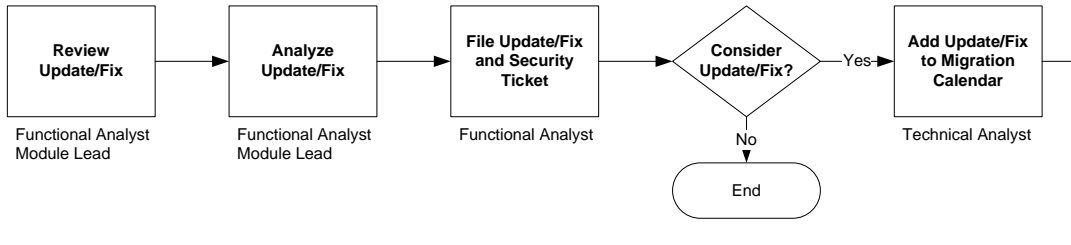
Update/Fix Announcement – ASG will send a notification to the appropriate functional analyst about each new update/fix posted to the CMS Systemwide website.

Update/Fix Status Review – ASG will review all updates/fixes for status updates as part of the weekly ASG Staff Meeting. This review will ensure no updates/fixes are ignored.

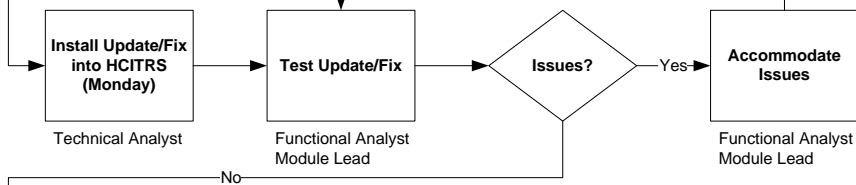
Update/Fix Status SharePoint Page – ASG will use SharePoint to list all updates/fixes for updates outside of the weekly ASG Staff Meeting. This page will provide a single point of reference for all updates/fixes.

4.0 Process Diagram

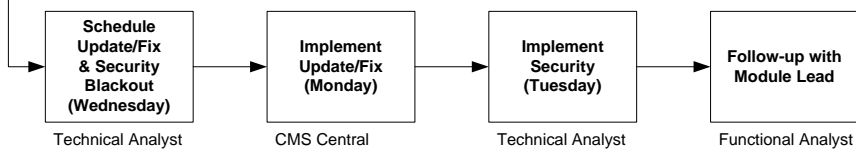
Phase 1 – Planning & Analysis



Phase 2 – Installation & Testing



Phase 3 – Implementation



5.0 Process Calendar

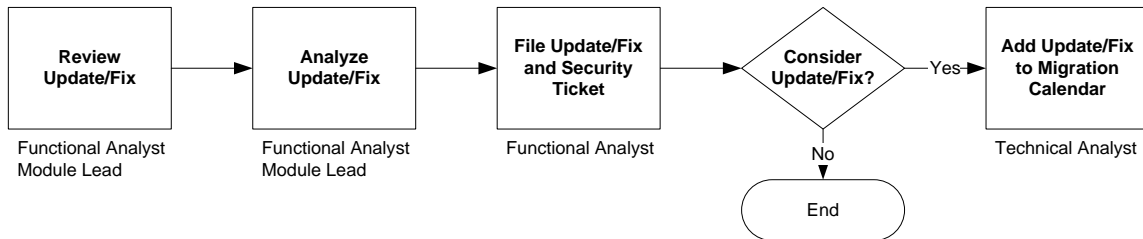
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
17	18	19	20	21	22	23
	Notification Sent	Analysis Begins				
24	25	26	27	28	29	1
	Analysis Ends Migration Evening	Install Begins				
2	3	4	5	6	7	8
	Install Ends	Testing Begins				
9	10	11	12	13	14	15
16	17	18	19	20	21	22
	Testing Check-in		G/NG Due Security Testing		All Testing Ends	
23	24	25	26	27	28	29
	Implemented Migration Evening	Security Applied			Follow-up to Module Lead	

Phase 1	Phase 2	Phase 3
---------	---------	---------

6.0 Phase 1 – Planning & Analysis

Phase 1 covers the planning and analysis of each update/fix. The Module Lead and Functional Analyst will review the update/fix to determine if it should be applied and produce an Update/Fix Analysis Document to describe the update/fix, produce testing scenarios, and compile any security impacts. The Functional Analyst will then file a ticket to track the update/fix. It is possible that a particular update/fix will not be considered until part of an upcoming Baseline Release package, and at this point the process ends while tracking the analysis portion. If the fix is to be scheduled, then the Technical Analyst will then install the update/fix in HCITRS and send a notification for testing.

6.1 Process Overview



6.2 Review Update/Fix

The Module Lead and Functional Analyst perform a high-level analysis on the impacted functionality. Most updates/fixes should be applied to our Production environment to ensure future pre-requisites are met.

Temporary Updates/Fixes

Updates/fixes may only be necessary until a future update, fix, or bundle is released by CMS Central. If an update/fix is temporary and does not affect current functionality, it may not need to be considered until the permanent update, fix, or bundle is released.

CMS Release Structure

CMS Releases are provided to bundle all PeopleSoft and CMS Systemwide updates, fixes, and enhancements into standard packages. If an update/fix is not required at the present time, and can wait until the next CMS Release, it may not need to be considered.

6.3 Analyze Update/Fix

Each update/fix should be analyzed for impacts on current functionality. All impacted functionality should be described and testing scenarios should be developed to provide comprehensive testing. All security impacts should be listed to help the Technical Analyst reserve enough time after implementation.

Current Functionality

Updates/fixes may impact future functionality delivered by CMS Central. Current functionality may not be affected by an update/fix, but it is possible portions of a particular update/fix may be required as future pre-requisites. If an update/fix impacts currently used objects, it should definitely be considered for implementation.

Update/Fix Analysis Document

Each update/fix must have an accompanying, completed Update/Fix Analysis Document, regardless of the size or impact of the update/fix. This document provides comprehensive information on how each update/fix will be tested and implemented. This document can be transferred to another staff member in the event the Module Lead, Functional Analyst, or Technical Analyst is unavailable. Each document will be stored on a shared drive to track progress and kept until each CMS Release has been installed that supersedes the previous updates/fixes.

6.4 File Update/Fix and Security Tickets

The Functional Analyst will file a ticket for the Technical Analyst to install the fix.

The completed Update/Fix Analysis Document should be attached and the following information should be provided for the installation ticket:

[Description]
Description: Update/Fix - HD91231 - AD - Mentor Updates
Update/Fix Posted: 9/1/2007

[Classification]
Type: Enterprise Applications
Subtype: PeopleSoft/CMS
Category: PT - Database

[Additional Items]
Action Required: CMS - Update/Fix
Technician Assigned: Q - CMS Technical
Update/Fix Needed: 9/26/2007
Module Lead: Jane Doe
Functional Analyst: John Doe
Pre-Requisites: <Listed>
Security Impacts: <Listed>
Special Considerations: <Listed>

The preliminary security documentation and the following information should be provided for the security ticket:

[Description]
Description: Update/Fix - HD91231 - AD - Mentor Updates
Update/Fix Posted: 9/1/2007

[Classification]
Type: Enterprise Applications
Subtype: PeopleSoft/CMS
Category: PT - System Access

[Additional Items]
Action Required: CMS - Security Request
Technician Assigned: Q - CMS Technical

Security Needed: 9/26/2007
Module Lead: Jane Doe
Functional Analyst: John Doe
Security Impacts: <Listed>

Non-CMS Testing Security

Some individuals outside of CMS Testing may require the global security currently assigned to CMS Testing members. Be sure to note those individuals when the security ticket is filed and make sure the Functional Analyst, Technical Analyst, and Module Lead are all notified of this need. This will expedite the process of assigning new functionality.

6.5 Add Update/Fix to Migration Calendar

The Technical Analyst will add the update/fix to the shared migration calendar. This decision is based upon the Update/Fix Analysis Document and feedback from the Functional Analyst and Module Lead.

Known Exceptions

Typically all updates/fixes will follow a three-week installation, testing, and implementation schedule. However, some regular updates released from CMS Central will knowingly not follow this process. See Appendix A for a list of known exceptions.

6.6 Deliverables/Milestones

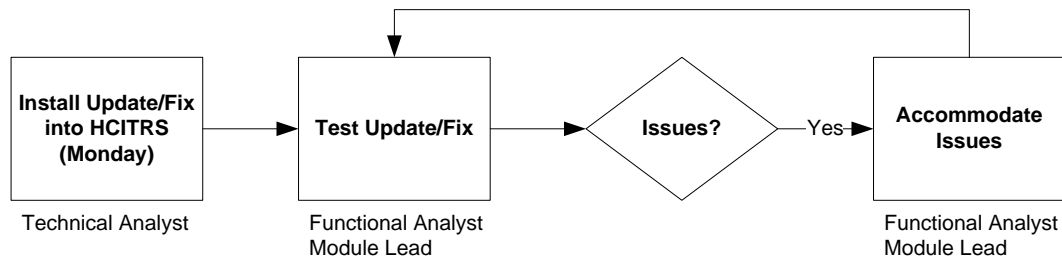
The following deliverables/milestones are required.

- *Update/Fix Analysis Document* – Completed documentation that provides a clear roadmap for installation, testing, and implementation.
- *Update/Fix Installation Ticket* – Ticket opened to the Technical Analyst to track all efforts to install and schedule the update/fix.
- *Updated Migration Calendar* – Migration calendar is updated to reflect the implementation schedule for the update/fix.

7.0 Phase 2 – Installation & Testing

Phase 2 covers the installation and testing of each update/fix. The Technical Analyst begins by installing all updates/fixes in HCITRS for the upcoming migration window. The Module Lead and Functional Analyst will utilize the update/fix analysis to test this update/fix and its security impacts. All issues should be logged and accommodated. Once testing has been completed, a notification is sent by the Functional Analyst to the Technical Analyst that this update/fix is ready for production.

7.1 Process Overview



7.2 Install Update/Fix into HCITRS

The Technical Analyst will install updates/fixes by Monday after processing security requirements and refreshes from the previous migration window. Most updates/fixes will not require more than one business day to install. After the update/fix has been installed and all security has been applied, a notification is sent back to the Module Lead and Functional Analyst for testing to begin.

Installation Timing

Update/fixes generally are installed, tested, and implemented over a three week period to provide adequate time for verification. Some updates/fixes may require longer timelines if they should be combined with other updates/fixes. Critical updates/fixes may accelerate this timeline with the proper justification. All efforts should be made to keep up with updates/fixes to ensure the timeline remains as consistent as possible.

7.3 Test Update/Fix

Each Update/Fix is tested according to the scenarios developed in the Update/Fix Analysis Document. The previous analysis should have identified all affected functionality. Once all issues have been resolved, the Functional Analysts sends a notice to the Technical Analyst.

Scheduling Timing

Critical updates/fixes can escalate the timeline with the necessary authorization and planning. Module Leads should contact the Functional Analyst and Technical Analyst for updates/fixes that will not meet this deadline to set the proper expectations. The final deadline for these critical updates/fixes will be Friday, 10am when we confirm our maintenance window. Updates/fixes received AFTER this timeline will require our Project Director to submit the business

justification to CMS Central. CMS Central reserves the right to deny late migration requests.

7.4 Accommodate Issues

Issues arising from this should be accommodated appropriately, potentially through data cleanup scripts, security adjustments, or workarounds depending on the severity of this update/fix.

Workarounds

Workarounds may be required for updates/fixes that are required as pre-requisites for functionality with a higher priority. Workarounds are temporary and issues that require them should be reported directly to CMS Central for resolution.

7.5 Deliverables/Milestones

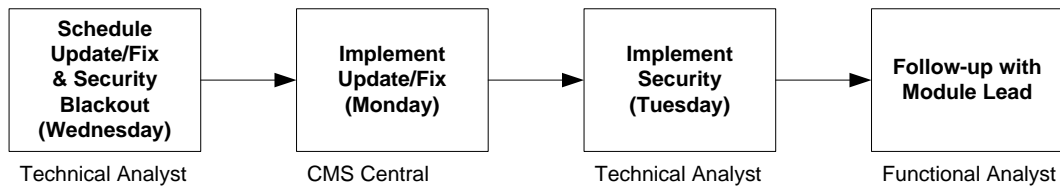
The following deliverables/milestones are required.

- *Update/Fix Testing Sign-Off* – Update/Fix Analysis Document is updated to include an official sign-off that the update/fix has been tested and is ready for implementation in Production.

8.0 Phase 3 – Implementation

Phase 3 covers the implementation of each update/fix. The Technical Analyst contacts CMS Central with all updates/fixes and campus enhancements that will be installed during a particular migration window. CMS Central installs all updates/fixes into Production during our regular maintenance night. The Technical Analyst the next morning implements any security changes. The Functional Analyst then contacts the Module Lead to acknowledge successful migration and follow-up with any issues.

8.1 Process Overview



8.2 Schedule Updates/Fixes / Security Blackout

All updates/fixes must be verified by the Wednesday prior to the Monday maintenance window. This allows the Technical Analyst and CMS Central to properly budget our maintenance window. Additionally, open security to new components will be removed in lieu of the completed security changes as determined during the analysis phase and developed during the testing phase. Exceptions are considered below.

Scheduling Timing

All updates/fixes will be installed during our Monday maintenance window. Only in extremely rare cases and with great business justification can we schedule on a night other than our scheduled night.

Scheduling Frequency

Our regular schedule will be every other Monday for migrations. This allows for more time and consistency for testing. All update/fix migrations will be suspended when preparing for a bundle/release installation. Only in extremely rare cases and with great business justification will be abandon this schedule. It is the job of the Functional Analyst and Module Lead to ensure their analysis of each update fix has taken this into consideration.

Security Testing

Functional Analysts should work with the Module Lead to determine all security changes (if any) were applied appropriately during the security blackout. All issues should be resolved prior to the Tuesday after migration.

8.3 Implement Updates/Fixes

Update/fix is installed by CMS Central during our regular maintenance window. We may only implement the number of updates/fixes that can be reasonably accommodated

(except in emergency situations) for each maintenance windows. CMS Central notifies the Technical Analyst about the completion of the maintenance window.

8.4 Implement Security

Any security requirements are implemented by the Technical Analyst. If there are no security requirements, then the Functional Analyst is notified of a successful migration. The Functional Analyst contacts the Module Lead and implements any workarounds or fixes to resolve issues identified in Phase 2.

Security Considerations

All security considerations should be finalized with accompanying change forms as necessary. Users may need to clear their browser cache to prevent as many issues as possible. Some security may not appear until Wednesday depending on the need for the Portal Sync process to run on Tuesday evening.

8.5 Follow-Up with Module Lead

The Functional Analyst contacts the Module Lead and implements any workarounds or fixes to resolve issues identified in Phase 2.

8.6 Deliverables/Milestones

The following deliverables/milestones are required.

- *Implemented Update/Fix*– CMS Central must complete the installation of the update/fix into Production. All participating roles should sign to declare their efforts in the process.
- *Implemented Security* – Technical Analyst must complete the security changes, if any.
- *Finalized Update/Fix Analysis Document* – Final documentation is signed-off to complete the update/fix installation.

Appendix A – Known Scheduling Exceptions

The following updates/fixes released by CMS Central are known exceptions to the standard three-week update/fix analysis and testing process. We will update this document with new items as they are identified. Please note that only updates/fixes that are routinely released in this manner should be released here. All critical fixes to broken functionality must still be accompanied by the necessary business justification.

Module	Functionality
Admissions	Mentor Functionality – Each year Mentor functionality is released two weeks prior to the first date of usage. A preview project is accompanied to perform the tested ahead of time. (October)
Finance / Student Financials	Year-End Reporting – CMS Central releases a bundle of updates/fixes for year-end reporting. This typically results in critical fixes being applied directly afterwards for final reporting. (June/July)
Finance / Student Financials	1098 Processing – CMS Central releases critical updates/fixes as issues are discovered for 1098 Processing. (January)
Finance / Student Financials	1099 Processing – CMS Central releases critical updates/fixes as issues are discovered for 1099 Processing. (January)