Texas Department of Public Safety
Change Request, CCB Meeting and Implementation Checklist

CHANGE REQUEST CHECKLIST

Completing a HEAT Change Request –

All **Standard** Change Requests (CR) are required to be submitted in ***Planned*** status by Friday by noon. QA and Technical meetings can be scheduled on Friday afternoon till Tuesday morning allowing time to complete the change request as described in this document. Completed CR is due on Tuesday by 2:30PM.

What	Due Date/Time
Planned Status	Friday 12:00PM
Ready for Review status and attachments	Tuesday 02:30PM
Presented at CCB	Wednesday 9:00AM

For details view the Process Flowchart

FYI and Maintenance CRs can go from ***Draft*** status to ***Ready for Review*** status.

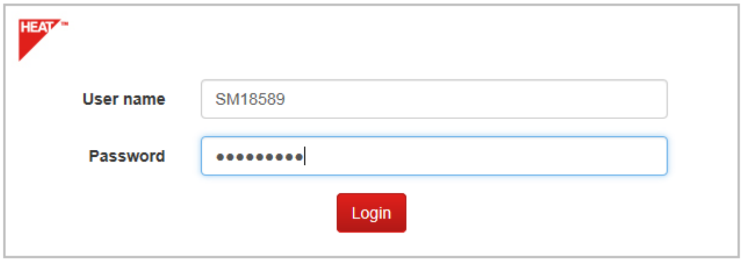
Before submitting a CR in ***Ready for Review*** status, please gather and attach the following documents to the change request:

Attach all IT Manager/Business approval (s)
Cyber scans need to be attached (when required)
Test results need to be attached (If you can't please specify why)
Implementation, validation and rollback plans
Operation manuals or support guide (if new or changed services requires operational support instructions, find instructions) Link to Operation Support Manuals
Notification to users (if the change has downtime or user impact)

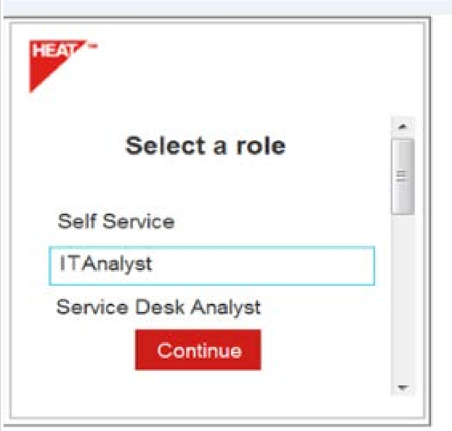
NOTE: Allow 2 hours for FYI and emergency change processing, find information and exceptions **here**

For additional information on CR artifacts please read CM-014 ITSM Change Request Artifacts Checklist .

SECTION 1 – HEAT LOGIN

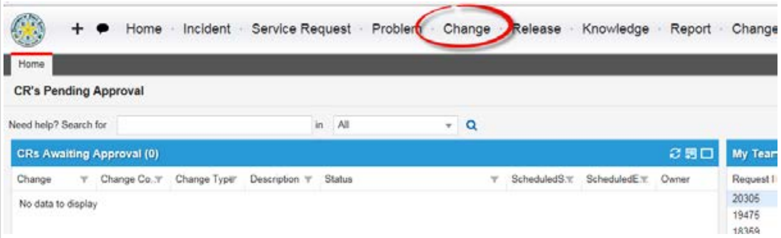
	Activity Needed - Outcome	***Detailed Steps to Complete***
□	1.1 Login to HEAT – (copy and paste link into your browser then press the enter key)	https://heat.tle.dps/HEAT/Default.aspx
□	1.2 Enter ACID and Network password	 User name SM18589 Password ••••••••• Click on the Login

□ 1.3 When logging in for the First time you will need to select a role.



Click on the Continue

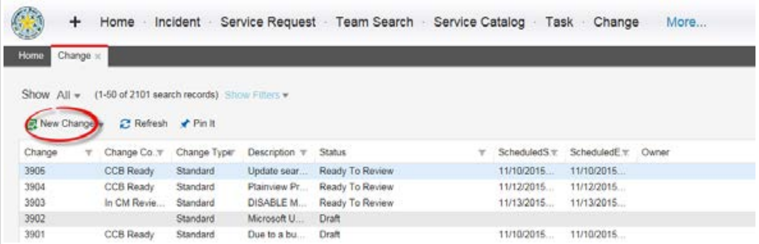
□ 1.4 Click on ***Change*** on the HEAT menu bar



Change	Change Co...	Change Type	Description	Status	ScheduledS...	ScheduledE...	Owner
No data to display							

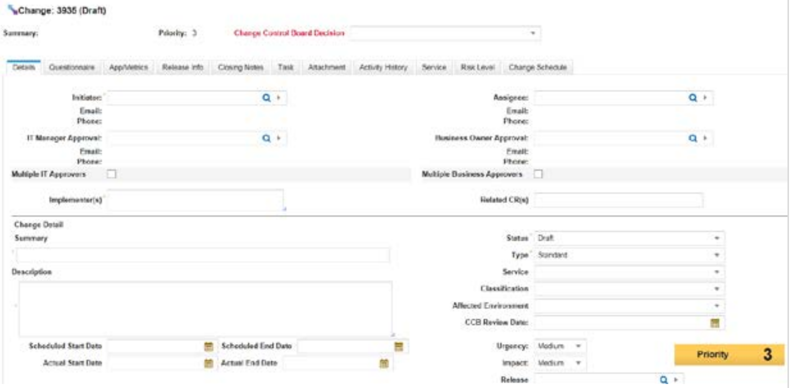
□ 1.5 Click on the ***New Change*** (Green Page icon) hyperlink

NOTE: The templates accessible from the dropdown are disabled.



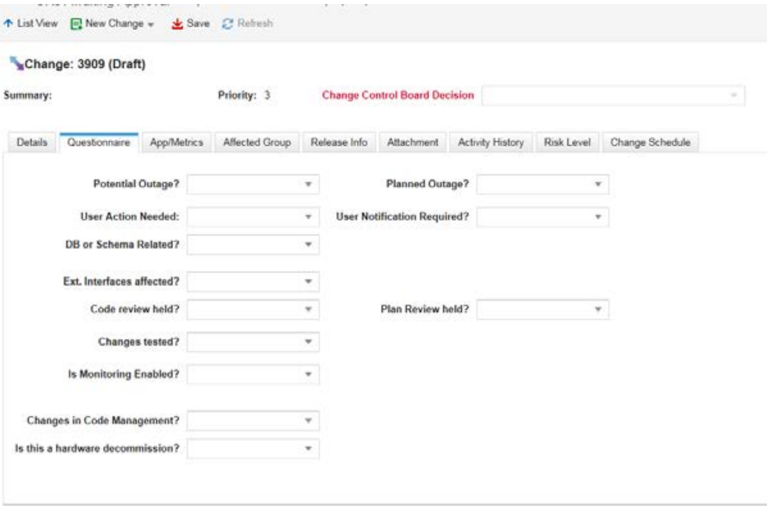
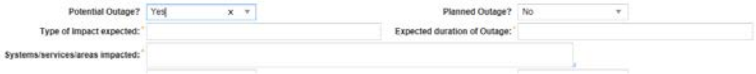
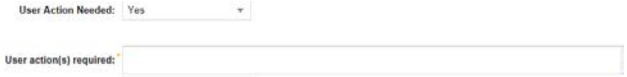
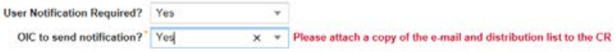
Change	Change Co...	Change Type	Description	Status	ScheduledS...	ScheduledE...	Owner
3905	CCB Ready	Standard	Update sear...	Ready To Review	11/10/2015...	11/10/2015...	
3904	CCB Ready	Standard	Plainview Pr...	Ready To Review	11/12/2015...	11/12/2015...	
3903	In CM Revie...	Standard	DISABLE M...	Ready To Review	11/13/2015...	11/13/2015...	
3902		Standard	Microsoft U...	Draft			
3901	CCB Ready	Standard	Due to a bu...	Draft	11/10/2015...	11/10/2015...	

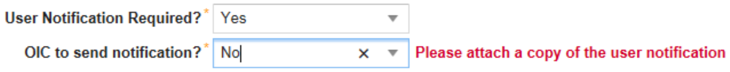
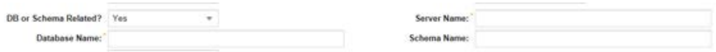
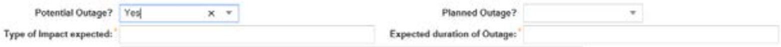
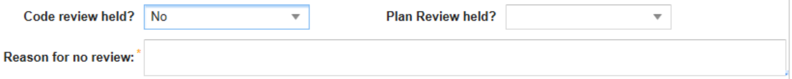
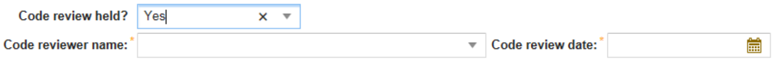
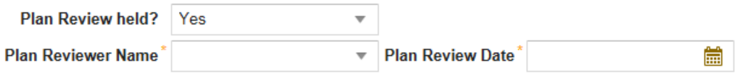
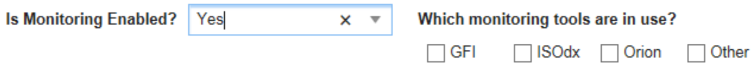
SECTION 2 – DETAIL TAB

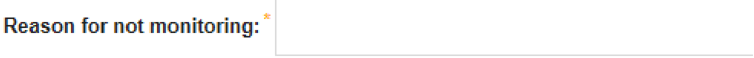
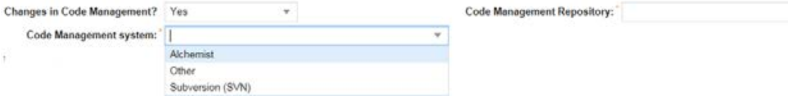
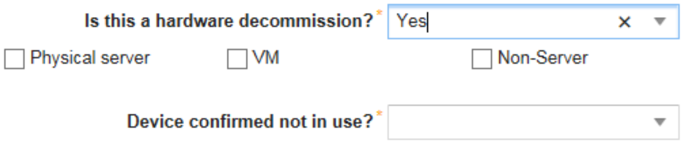
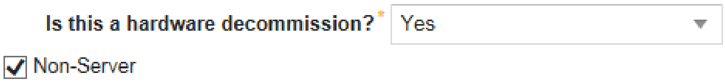
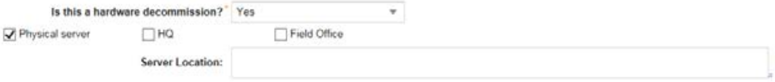
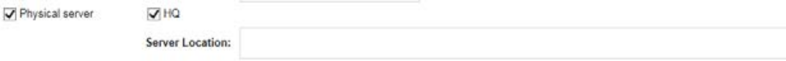
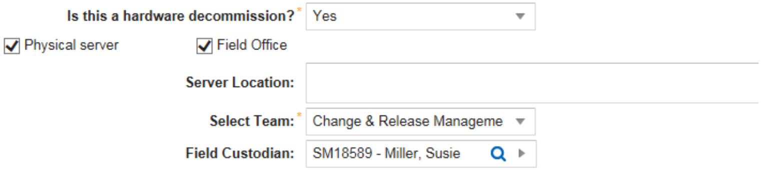
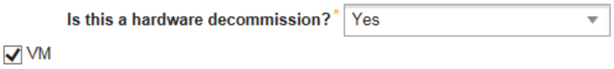
	Activity Needed - Outcome	*Detailed Steps to Complete*
☐	2.1 ***Detail*** Tab: The **Detail** page is used to: - document name and information for the initiator, approvers, implementers - document a summary of the change - document the details for the change o Provide detailed description of the change, problem, circumstance leading to the requested change o Include the reason why the change has been requested and the justification for the request - document the schedules of the release - document the system, environment, classification, service, urgency, and impact - document the CCB decision Your name is the default for the Initiator and Assignee fields. If necessary, change the default names to the person(s) responsible.	 Change: 3935 (Draft) Priority: 3 Status: Draft Type: Standard Urgency: Medium Impact: Medium Priority 3 Summary: Change Control Board Decision Details Questionnaire App/Metrics Release Info Closing Notes Task Attachment Activity History Service Risk Level Change Schedule Initiator: Email: Phone: Assignee: Email: Phone: IT Manager Approval: Email: Phone: Business Owner Approval: Email: Phone: Multiple IT Approvers Multiple Business Approvers Implementer(s) Related CR(s) Change Detail Summary Description Service Classification Affected Environment CCB Review Date: Scheduled Start Date Scheduled End Date Actual Start Date Actual End Date Release Fig - 1 For more details see CM-019 CR Review Process, Detail Tab section starting on page 15
	2.2 Enter the name manager who approved the change in the ***IT Manager Approval*** field (see Fig 1)	IT Manager Approval is a required field. The IT managers of the affected areas and the managers of the implementers (if other than the affected areas) must approve the CR.
	2.3 Enter the name manager who approved the change in the ***Business Owner Approval*** (see Fig 1)	The Business Owner of the affected areas and the managers of the implementers (if other than the affected areas) must approve the CR.
☐	2.4 ***Multiple IT Approvers (if needed)*** (see Fig 1)	If the CR change requires more than one manager approval, the box should be checked and the additional IT Manager(s) should be listed. This field becomes required as soon as the box is checked. **Note**: All Change Requests require both an IT and Business Approver and these must be different managers.
☐	2.5 ***Summary*** (see Fig 1)	Enter a brief and meaningful CR summary
☐	2.6 ***Description*** (see Fig 1)	Enter a detailed description, reason/purpose for the change. For example: What is the change going to accomplish? If there is more than one change list each change required. What is the problem being fixed.
☐	2.7 ***Scheduled Start Date and Time*** (see Fig 1)	Enter the date and time for the CR. Please keep in mind the OIC changes shifts at 7:00 am and 7:00 pm. Any changes during this time should be 15 minutes before or after 7:00.
☐	2.8 ***Scheduled End Date and Time*** (see Fig 1)	Enter the date and time the CR is expected to be complete. Please keep in mind the OIC changes shifts at 7:00 am and 7:00 pm. Any changes during this time should be 15 minutes before or after 7:00.

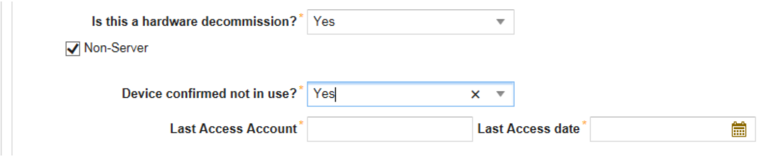
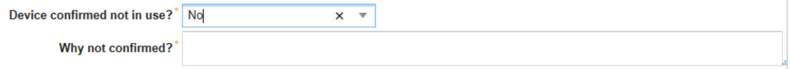
□	2.9 ***Status*** (see Fig 1) **NOTE**: *The status field is used to submit the CR to Change Management for processing.*	The default status is ***Draft.*** FYI and Maintenance CRs -- Status should be set to ***Ready for Review*** after all artifacts have been attached. Standard CRs -- Change the status to ***Planned.*** All planned standard CRs will be reported on in the DPS – Planned Change Report and sent every Friday at 2:00pm. Recipients of the report will review the items on the agenda and schedule meetings as needed. When ready, the CR should be completely filled out including the A.C.T.I.O.N items and status should be changed to ***Ready for Review***. The due date for a completed CR is Tuesday by 2:30PM. A validation check on the required fields will be conducted by HEAT automatically and inform you of any missing required information. Change Management will review the CR prior to adding it to the Change Control Board (CCB) agenda to ensure it is complete and ***Ready for Review*** by the CCB members. For more details see CM-019 CR Review Process, Detail Tab section starting on page 16
□	2.10***CR Type*** (see Fig 1)	Standard, FYI, Emergency, Maintenance For more details see CM-019 CR Review Process, CR types section, starting on page 5 for the descriptions for each type and see page 16 for more information on the CR type field.
□	2.11 ***Service*** (see Fig 1)	Select the appropriate service from the Service dropdown
□	2.12 ***Classification*** (see Fig 1)	Select the appropriate classification: (None, Enhancement, Incident/Problem, Release, Scheduled Maintenance, Unscheduled Maintenance)
□	2.13 ***Affected Environment*** (see Fig 1)	Select the environment that is affected by the change (Production, Test, Development, Pilot, and QA).
□	2.14 ***CCB Review Date*** (see Fig 1)	Enter the upcoming CCB review date for Standard and Maintenance CR types. **Note**: The CCB meets every Wednesday with exceptions during holidays; Change Management will send notifications for cancelled or rescheduled meetings. The Outlook calendar invitation and agenda emails contain the conference room locations, conference bridge information, and WebEx meeting information. See CM-000 Change Management Policies and Procedures, Change Control Board section page 11.
□	2.15 ***Urgency***(see Fig 1)	Select the appropriate Urgency (High, Medium, Low) to assist in making this determination see CM-019 CR Review Process, page 17
□	2.16 ***Impact*** (see Fig 1)	Select the appropriate Impact (High, Medium, Low) to assist in making this determination see CM-019 CR Review Process, page 17
□	2.17 ***Release*** (see Fig 1)	Not currently used.
□	2.18 To save the CR in the current state click on the Save link	
Continue to completing the Questionnaire tab section next…		

SECTION 3 – QUESTIONNAIRE TAB

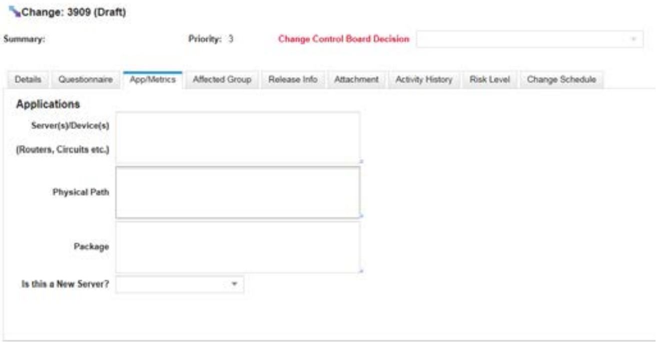
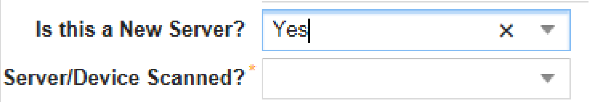
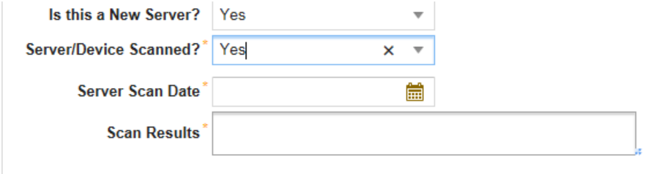
	Activity Needed - Outcome	***Detailed Steps to Complete***
☐	3.1 The ***Questionnaire*** tab The Questionnaire page is used to: • document any potential/planned outages • identify users affected and actions they may need to take • list external interfaces that may be impacted by the change • document the code and/or peer review • document the testing of the change • Indicate which monitoring tool used • Document where the code is stored All questions on the Questionnaire page must be answered. **Note**: The questionnaire page contains hidden fields that are conditionally required. These fields are dependent on responses made to the main questions on the page.	 List View · New Change · Save · Refresh Change: 3909 (Draft) Summary: Priority: 3 Change Control Board Decision Details · Questionnaire · App/Metrics · Affected Group · Release Info · Attachment · Activity History · Risk Level · Change Schedule Potential Outage? Planned Outage? User Action Needed: User Notification Required? DB or Schema Related? Ext. Interfaces affected? Code review held? Plan Review held? Changes tested? Is Monitoring Enabled? Changes in Code Management? Is this a hardware decommission? Fig 2 For more details see [CM-019 CR Review Process]() Questionnaire Tab section starting on page 21
☐	3.2 ***Potential Outage*** (see Fig 2)	Is there a risk for an uplanned outage or downtime? If so enter the information in this field.
☐	3.3 ***Planned Outage*** (see Fig 2)	Select (Yes/No)
☐	3.4 **Yes** response	When a **Yes** response is indicated on either the ***Potential Outage*** or ***Planned Outage*** the following questions become required: • ***Type of Impact expected*** • ***Expected duration of Outage*** • ***Systems/services/areas impacted***  Potential Outage? Yes Planned Outage? No Type of Impact expected:* Expected duration of Outage:* Systems/services/areas impacted:*
☐	3.5 ***User Action Needed*** (see Fig 2)	Select (Yes/No) Do uses need to take action for this change? If **Yes**, the user action required field will be required.
☐	3.6 **Yes** response	When a **Yes** response is indicated the following question will be required. • ***User action required*** • ***User Notification Required*** will default to ***Yes*** Describe the actions the user must take. User notification will be required when user actions are needed.  User Action Needed: Yes User action(s) required:* When user notification is required a second question will display asking if the OIC is to send out the notification. When a ***Yes*** response is indicated a message will display reminding you to attach a copy of the e-mail and the distribution list.  User Notification Required? Yes OIC to send notification?* Yes Please attach a copy of the e-mail and distribution list to the CR If the answer is ***No*,** a message will display reminding the initiator to

		attach a copy of the email notification to the CR.  User Notification Required?* Yes OIC to send notification?* No Please attach a copy of the user notification
□	3.7 ***User Notification Required?*** (see Fig 2)	If user notification is required you will need to attach a copy of the notification to the CR. See Attachment section for additional information.
□	3.9 ***DB or Schema Related?*** (see Fig 2)	If DB or schema changes are impacted by the change additional required fields will become visable. All additional questions will need to be completed.
□	3.10 **Yes** response	Database Name, Server Name and Schema Name become required  DB or Schema Related? Yes Database Name:* Server Name:* Schema Name:
□	3.11 ***Ext. Interfaces affected?*** (see Fig 2)	Select (Yes/No)
□	3.12 ***Yes*** response	Interfaces/Applications and Type of Effect will become required fields  Potential Outage? Yes Type of Impact expected:* Planned Outage? Expected duration of Outage:*
□	3.13***Code Review held?*** (see Fig 2)	Responses (Yes/No/NA) If the response is No, the Reason for no review question will become required. **NOTE**: See CM-019 CR Review Processpage 23 – 24 for information on Code and Peer Reviews
□	3.14 ***No*** response	 Code review held? No Plan Review held? Reason for no review:*
□	3.15 ***Yes*** response	 Code review held? Yes Code reviewer name:* Code review date:*
□	3.16 ***Plan Review held?*** (see Fig 2)	Select (Yes/No/NA) **NOTE**: A plan review will become required if a code review is not applicable.
□	3.17 ***Yes*** response	 Plan Review held? Yes Plan Reviewer Name* Plan Review Date*
□	3.18 ***Changes Tested? (see Fig 2)***	Select (Yes/No/NA) **NOTE**: See CM-019 CR Review Process page 25 for additional information
□	3.19 ***Yes*** response	Location of Test results and date tested fields become requied
□	3.20 ***No*** response	***Reason for not testing*** becomes required. See CM-11 ITSM Terminology and Test Results Guidelines for assistance in completing this field. **NOTE**: Validation artifacts will be required, when approprate, for all CRs that could not be tested.
□	3.21***Is Monitoring Enabled?*** (see Fig 2)	Select (Yes/No/NA)
□	3.22 ***Yes*** response	Monitoring tools used will become required  Is Monitoring Enabled? Yes Which monitoring tools are in use? □ GFI □ ISOdx □ Orion □ Other

☐	3.23 ***No*** response	Reason for not monitoring field will become required  Reason for not monitoring:*
☐	3.24 ***Changes in Code Management?*** (See Fig 2)	Select (Yes/No/NA)
☐	3.25 ***Yes*** response	Code Management system and Code Management Repository become required fields Select the Code Management system from the dropdown box and paste a code location link to the Code Management Repository field  Changes in Code Management? Yes Code Management Repository:* Code Management system:*
☐	3.26 ***Is this a hardware decommission?* (see Fig 2)**	Select (Yes/No)
☐	3.27 ***Yes*** response	Will trigger 3 checkboxes to indicate what type of hardware decommission the change is for and will display the Device confirmed not in use question.  Is this a hardware decommission?* Yes ☐ Physical server ☐ VM ☐ Non-Server Device confirmed not in use?* See [CM-019 CR Review Process]() page 26 for information
	3.28 **Selecting Non-Server**	Will hide the Physical and VM checkboxes.  Is this a hardware decommission?* Yes ☑ Non-Server
	3.29 **Selecting Physical Server**	Will display addtion additional fields.  Is this a hardware decommission?* Yes ☑ Physical server ☐ HQ ☐ Field Office Server Location:
	3.30 **Selecting HQ**	Will hide the Field Office checkbox. Enter the server location:  ☑ Physical server ☑ HQ Server Location:
	3.31 **Selecting Field**	Will hide the HQ and display additional fields that will be required. Enter the Server Location Select Team Select Custodian  Is this a hardware decommission?* Yes ☑ Physical server ☑ Field Office Server Location: Select Team:* Change & Release Manageme Field Custodian: SM18589 - Miller, Susie
	3.32 **Select VM**	A VM decommission will not have additional questions. Go to the next question.  Is this a hardware decommission?* Yes ☑ VM

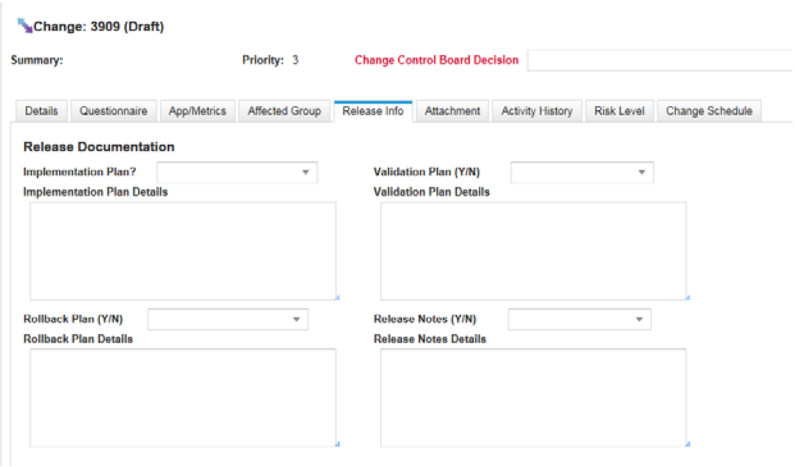
	3.33 **Device confirmed not in use? Yes response**	The Device confirmed not in use answer will trigger additional questions which are dependant on the Yes/No response. Will display the “Last Access Account” and “Last Access date” questions. Enter the ACID or name of the person who last accessed the server and the date.  Is this a hardware decommission?* Yes ☑ Non-Server Device confirmed not in use?* Yes Last Access Account* Last Access date*
	3.34 **Device confirmed not in use? No response**	Will display the “Why not confirmed?” required question. Enter the reason why it was not confirmed.  Device confirmed not in use?* No Why not confirmed?*
□	3.35 To save the CR in the current state click on the Save link	
Continue to completing the App/Metrics tab section next…		

SECTION 4 – APP/METRICS TAB

	Activity Needed – Outcome	*Detailed Steps to Complete*
☐	4.1 ***Applications and Metrics*** page The App/Metrics tab is used to document which servers, devices or applications are impacted by the change as well as the file location and package names that are used for the change. In addition, information on new servers and devices is documented on this page.	 Change: 3909 (Draft) Summary: Priority: 3 Change Control Board Decision Details Questionnaire App/Metrics Affected Group Release Info Attachment Activity History Risk Level Change Schedule Applications Server(s)/Device(s) (Routers, Circuits etc.) Physical Path Package Is this a New Server? **Fig 3** See CM-019 CR Review Process page 28 for information on the App/Metrics Tab
☐	4.2 ***Server(s) Devices (s) Routers, Circuits etc.*** (see Fig 3)	Enter the names of the impacted devices in this field
☐	4.3 ***Physical Path*** (see Fig 3)	Enter the physical path impacted by the change
☐	4.4 ***Packages*** (see Fig 3)	Enter the package names in this field
☐	4.5 ***Is this a new Server?*** (see Fig 3)	Select (Yes/No) NOTE: If the question "Is this a hardware decommission?" is Yes this question will be hidden.
☐	4.6 ***Yes*** response	Triggers the Server/Devices Scanned question Is this a New Server? Yes Server/Device Scanned?*
☐	4.7 ***Server/Device Scanned?*** 4.8 ***Yes*** response	Triggers the Server Scan Date and Results questions both are required fields Is this a New Server? Yes Server/Device Scanned?* Yes Server Scan Date* Scan Results*
☐	4.9 To save the CR in the current state click on the Save link	

Continue to completing the Release Info tab section next…

SECTION 5 – RELEASE INFO TAB

	Activity Needed - Outcome	*Detailed Steps to Complete*
☐	5.1 ***Release Info*** Tab This form is used to document the release information such as Implementation Plans, Rollback Plan and Validation Plan which are all required for the completion of a CR. Acceptable responses are **Yes** or **No**. If "**No"** is selected, a justification must be provided in the text box indicating why the documentation is not provided.	 Change: 3909 (Draft) Priority: 3 Summary: Change Control Board Decision Details Questionnaire App/Metrics Affected Group Release Info Attachment Activity History Risk Level Change Schedule Release Documentation Implementation Plan? Implementation Plan Details Validation Plan (Y/N) Validation Plan Details Rollback Plan (Y/N) Rollback Plan Details Release Notes (Y/N) Release Notes Details Fig 4 See CM-019 CR Review Process page 31 for information on the Release Info Tab
☐	5.2 ***Implementation Plan and Details*** (see Fig 4)	The steps for implementing the changes on the CR should be listed here. **Special note:** All implementation plans begin with a call to OIC to put the CR in progress. OIC is responsible for entering the Actual start and end times on the CR. This action also enables the CR to be closed once complete.
☐	5.3 ***Rollback Plan and Details*** (see Fig 4)	All CRs should document the rollback plan.
☐	5.4 ***Validation Plan and Details*** (see Fig 4)	An explanation of how the changes will be validated should be included on all CRs.
☐	5.5 ***Release Notes (Y/N)*** (see Fig 4)	**NOTE**: Required on all new systems and applications releases or updates to applications. See CM-019 CR Review Process page 32 for information
☐	5.6 At this point, the Change Request status should be reviewed and updated according to the Change Request Type	Click on the ***Details*** Tab For FYI, Maintenance and Emergency changes change the ***Status*** from ***Draft*** to ***Ready for Review.*** A validation check on the required fields will be conducted by HEAT automatically and inform you of any missing required information. For Standard change the status from ***Draft*** to ***Planned.*** All planned standard CRs will be reported on in the DPS – Planned Change Report and sent every Friday at 2:00pm. Recipients of the report will review the items on the agenda and schedule meetings as needed. When ready, the CR should be completely filled out including the A.C.T.I.O.N items and status should be changed to ***Ready for Review.*** The due date for a completed CR is Tuesday by 2:30PM. A validation check on the required fields will be conducted by HEAT automatically and inform you of any missing required information. The ***Change Control Board Decision*** field will be populated with ***Awaiting Approval***. Change Management will review the CR prior to adding it to the Change Control Board agenda to ensure it is complete and ***Ready for Review*** by the Change Control Board members. If it is missing any data CR reviewer will change the ***Change Control Board***

		Decision to ***In CM Review Pending Update***. Once all artifacts are received the CR reviewer will change the ***Change Control Board Decision*** to ***CCB Ready*.** This ensures the CR is ready to be reviewed at the CCB meeting. For more details see CM-019 CR Review Process Detail Tab section starting on page 16
□	5.7 To save the CR in the current state click on the Save link	Click on Save

CLOSING NOTES TAB

See Implementation Checklist section
If you have attachments to be added to the CR go to the Attachment Tab section next

SECTION 6 – ATTACHMENT TAB

Activity Needed - Outcome

Detailed Steps to Complete

☐ 6.1 ***Attachment*** Tab

The attachment page is used to upload artifacts such as supporting files, e-mails, approvals, artifacts, validation screenshots, test results, URLs, or other types of notes.

Attach all IT Manager/Business approval (s) listed on the CR

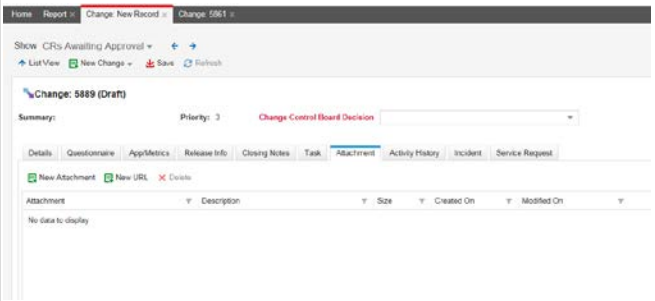
Cyber scans need to be attached (when required)

Test results need to be attached (If you can't please specify why)

I Implementation, validation and rollback plans

Operation manuals or support guide (as needed)

Notification to users (if the change has downtime or user impact)



Change: 5889 (Draft)

Summary:

Priority: 3

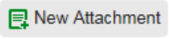
Change Control Board Decision

Attachment	Description	Size	Created On	Modified On
No data to display				

See CM-019 CR Review Process page 32 for detailed information

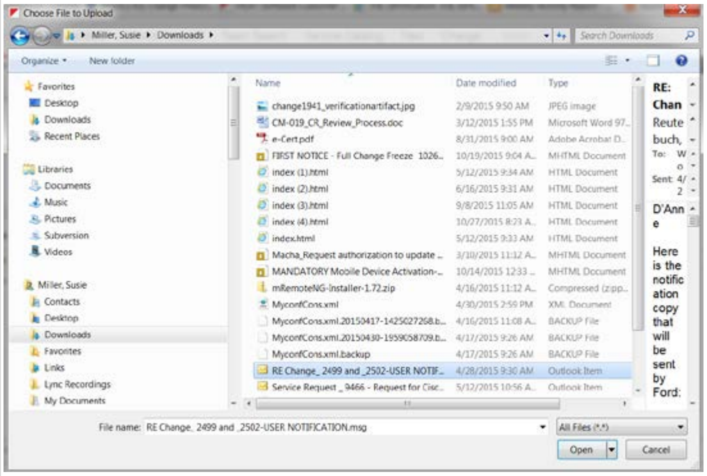
6.2 Adding an email, document, or other attachment

Click on ***New Attachment***



The ***Choose File to Upload*** window will open.

Select the doucment



Name	Date modified	Type
change1941_verificationartifact.jpg	2/9/2015 9:50 AM	JPEG image
CM-019_CR_Review_Process.doc	3/12/2015 1:55 PM	Microsoft Word 97...
e-Cert.pdf	8/31/2015 9:00 AM	Adobe Acrobat D...
FIRST NOTICE - Full Change Freeze 1026...	10/19/2015 9:04 A...	MHTML Document
index (1).html	5/12/2015 9:34 AM	HTML Document
index (2).html	6/16/2015 9:31 AM	HTML Document
index (3).html	9/8/2015 11:05 AM	HTML Document
index (4).html	10/27/2015 8:23 A...	HTML Document
index.html	5/12/2015 9:33 AM	HTML Document
Macha_Request authorization to update ...	3/10/2015 11:12 A...	MHTML Document
MANDATORY Mobile Device Activation-...	10/14/2015 12:33 ...	MHTML Document
mRemoteNG-Installer-1.72.zip	4/16/2015 11:12 A...	Compressed (zipp...
MyconfCons.xml	4/30/2015 2:59 PM	XML Document
MyconfCons.xml.20150417-1425027268.b...	4/16/2015 11:08 A...	BACKUP File
MyconfCons.xml.20150430-1959058709.b...	4/17/2015 9:26 AM	BACKUP File
MyconfCons.xml.backup	4/17/2015 9:26 AM	BACKUP File
RE Change_ 2499 and _2502-USER NOTIF...	4/28/2015 9:30 AM	Outlook Item
Service Request _ 9466 - Request for Cisc...	5/12/2015 10:56 A...	Outlook Item

RE: Chan Reute buch, To: W o Sent: 4/ 2 D'Ann e Here is the notific ation copy that will be sent by Ford:

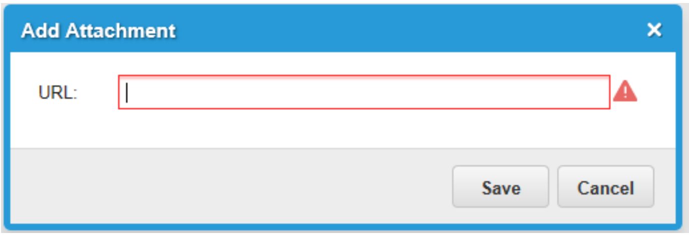
File name: RE Change_2499 and _2502-USER NOTIFICATION.msg

All Files (*.*)

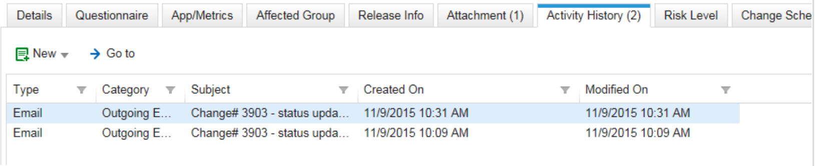
Click on Open

☐ 6.3 Adding a URL attachment

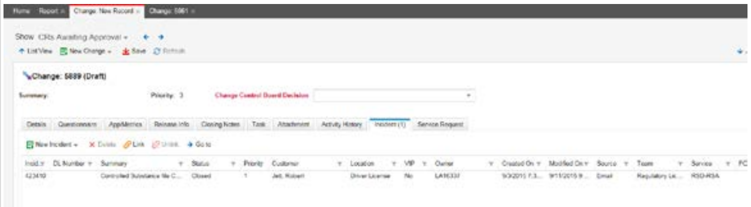
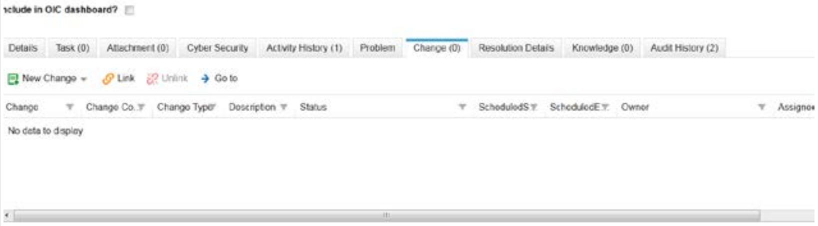
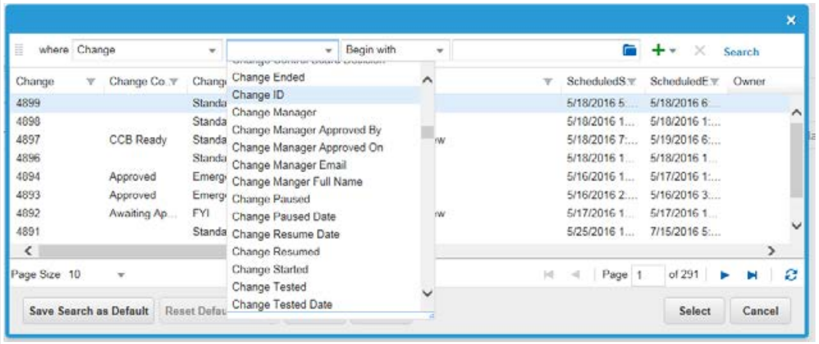
Click on ***New URL*** and paste the URL in the field and click on Save



ACTIVITY HISTORY TAB

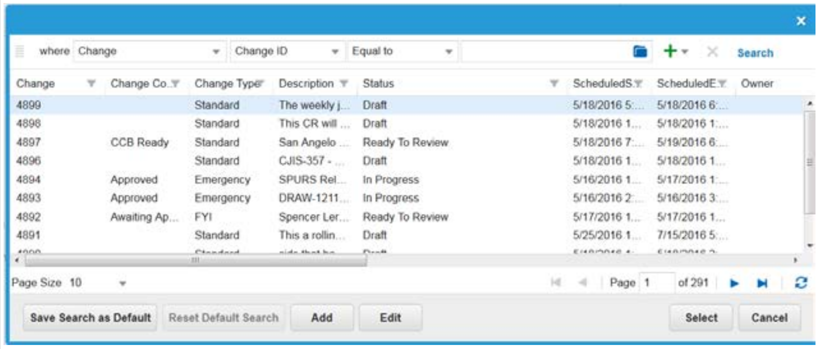
	Activity Needed - Outcome	Detailed Steps to Complete
☐	7 ***Activity History*** Tab The Activity History page tracks email activity related to a CR, which is usually initiated by business rules within the HEAT system. Although it is seldom used, functionality allows users to add notes to the CR or generate an email from the HEAT system to track external CR activities.	 Details Questionnaire App/Metrics Affected Group Release Info Attachment (1) Activity History (2) Risk Level Change Sche New Go to Type | Category | Subject | Created On | Modified On Email | Outgoing E... | Change# 3903 - status upda... | 11/9/2015 10:31 AM | 11/9/2015 10:31 AM Email | Outgoing E... | Change# 3903 - status upda... | 11/9/2015 10:09 AM | 11/9/2015 10:09 AM

INCIDENT TAB

	Activity Needed - Outcome	Detailed Steps to Complete
☐	8 ***Incident*** Tab The Incident tab is used to link an existing incident that is related to or resulted in the change to the change request. Select Incident tab	 Home Report Change: New Record Change: 5861 Show CRs Awaiting Approval List View New Change Save Refresh Change: 5889 (Draft) Summary: Priority: 3 Change Control Board Decision Details Questionnaire App/Metrics Release Info Closing Notes Task Attachment Activity History Incident (1) Service Request New Incident Delete Link Unlink Go to Incid | DL Number | Summary | Status | Priority | Customer | Location | VIP | Owner | Created On | Modified On | Source | Team | Service | FC 423410 | | Controlled Substance Ne C... | Closed | 1 | Jett, Robert | Driver License | No | LA16337 | 9/3/2015 7:3... | 9/11/2015 9:... | Email | Regulatory Lic... | RSD-RSA
☐	**9** Select Link	 nclude in OIC dashboard? Details Task (0) Attachment (0) Cyber Security Activity History (1) Problem Change (0) Resolution Details Knowledge (0) Audit History (2) New Change Link Unlink Go to Change | Change Co... | Change Type | Description | Status | ScheduledS | ScheduledE | Owner | Assignee No data to display
☐	10 You will need to select the following from the drop down menu: " Change, Change ID, Equal to" then enter the CR #	 where Change Begin with Search Change Ended Change ID Change Manager Change Manager Approved By Change Manager Approved On Change Manager Email Change Manger Full Name Change Paused Change Paused Date Change Resume Date Change Resumed Change Started Change Tested Change Tested Date Page Size 10 Page 1 of 291 Save Search as Default Reset Defau Select Cancel Change | Change Co... | Chang... | ScheduledS | ScheduledE | Owner 4899 | | Standa | 5/18/2016 5:... | 5/18/2016 6:... 4898 | | Standa | 5/18/2016 1... | 5/18/2016 1:... 4897 | CCB Ready | Standa | 5/18/2016 7:... | 5/19/2016 6:... 4896 | | Standa | 5/18/2016 1... | 5/18/2016 1... 4894 | Approved | Emerg | 5/16/2016 1... | 5/17/2016 1:... 4893 | Approved | Emerg | 5/16/2016 2:... | 5/16/2016 3:... 4892 | Awaiting Ap... | FYI | 5/17/2016 1... | 5/17/2016 1... 4891 | | Standa | 5/25/2016 1... | 7/15/2016 5:...

☐ 11

Highlight the record that you want to link (change or incident) and click “Select”.
The screen shot is an example of linking a change request to an incident record



where Change | Change ID | Equal to | Search

Change	Change Co..	Change Type	Description	Status	ScheduledS..	ScheduledE..	Owner
4899		Standard	The weekly j...	Draft	5/18/2016 5:...	5/18/2016 6:...	
4898		Standard	This CR will ...	Draft	5/18/2016 1...	5/18/2016 1:...	
4897	CCB Ready	Standard	San Angelo ...	Ready To Review	5/18/2016 7:...	5/19/2016 6:...	
4896		Standard	CJIS-357 - ...	Draft	5/18/2016 1...	5/18/2016 1...	
4894	Approved	Emergency	SPURS Rel...	In Progress	5/16/2016 1...	5/17/2016 1:...	
4893	Approved	Emergency	DRAW-1211...	In Progress	5/16/2016 2:...	5/16/2016 3:...	
4892	Awaiting Ap...	FYI	Spencer Ler...	Ready To Review	5/17/2016 1...	5/17/2016 1...	
4891		Standard	This a rollin...	Draft	5/25/2016 1...	7/15/2016 5:...	

Page Size 10 | Page 1 of 291

Save Search as Default | Reset Default Search | Add | Edit | Select | Cancel

See CM-051 CR and Incident Linking for more information

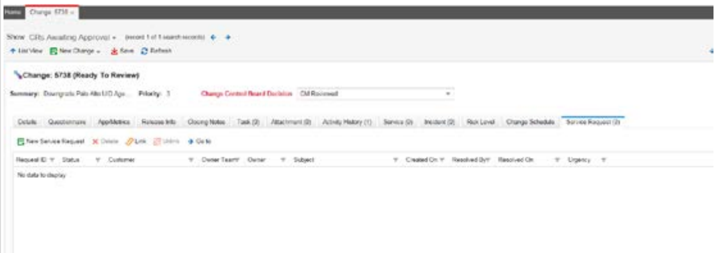
SERVICE REQUEST TAB

Activity Needed - Outcome | ***Detailed Steps to Complete***

☐ ***11*** ***Service Request*** Tab

The Service Request tab is used to link an existing Service Request that is related to or resulted in the change to the change request.

Select Service Request tab



Home | Change 5738

Show CRs Awaiting Approval (record 1 of 1 search records)

List View | New Change | Save | Refresh

Change: 5738 (Ready To Review)

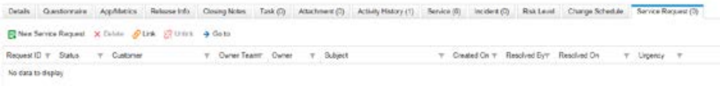
Summary: Downgrade Palo Alto UID Age... Priority: 1 Change Control Board Decision: CM Reviewed

Details | Questionnaire | App/Metrics | Release Info | Closing Notes | Task (0) | Attachment (0) | Activity History (1) | Service (0) | Incident (0) | Risk Level | Change Schedule | Service Request (0)

New Service Request | Delete | Link | Unlink | Go to

Request ID	Status	Customer	Owner Team	Owner	Subject	Created On	Resolved By	Resolved On	Urgency
No data to display									

☐ ***12*** Select Link

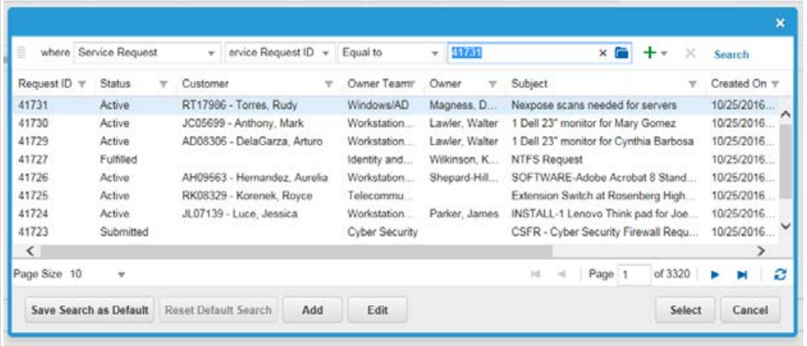


Details | Questionnaire | App/Metrics | Release Info | Closing Notes | Task (0) | Attachment (0) | Activity History (1) | Service (0) | Incident (0) | Risk Level | Change Schedule | Service Request (0)

New Service Request | Delete | Link | Unlink | Go to

Request ID	Status	Customer	Owner Team	Owner	Subject	Created On	Resolved By	Resolved On	Urgency
No data to display									

☐ ***13*** You will need to select the following from the drop down menu: “ Service Request, Request ID, Equal to” then enter the SR # and Click on the blue Search link



where Service Request | ervice Request ID | Equal to | 41731 | Search

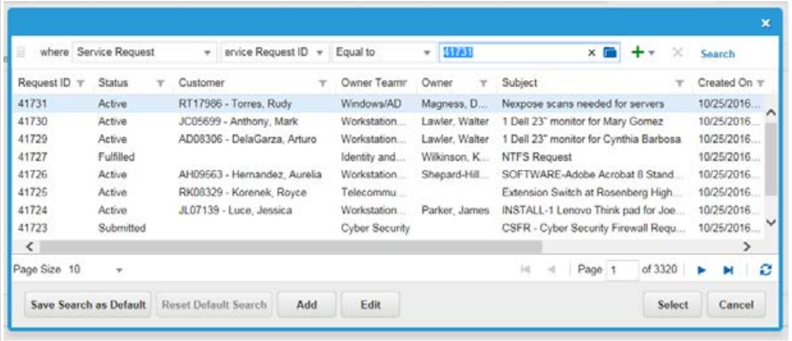
Request ID	Status	Customer	Owner Team	Owner	Subject	Created On
41731	Active	RT17986 - Torres, Rudy	Windows/AD	Magness, D...	Nexpose scans needed for servers	10/25/2016...
41730	Active	JC05699 - Anthony, Mark	Workstation...	Lawler, Walter	1 Dell 23" monitor for Mary Gomez	10/25/2016...
41729	Active	AD08306 - DelaGarza, Arturo	Workstation...	Lawler, Walter	1 Dell 23" monitor for Cynthia Barbosa	10/25/2016...
41727	Fulfilled		Identity and...	Wilkinson, K...	NTFS Request	10/25/2016...
41726	Active	AH09563 - Hernandez, Aurelia	Workstation...	Shepard-Hill...	SOFTWARE-Adobe Acrobat 8 Stand...	10/25/2016...
41725	Active	RK08329 - Korenek, Royce	Telecommu...		Extension Switch at Rosenberg High...	10/25/2016...
41724	Active	JL07139 - Luce, Jessica	Workstation...	Parker, James	INSTALL-1 Lenovo Think pad for Joe...	10/25/2016...
41723	Submitted		Cyber Security		CSFR - Cyber Security Firewall Requ...	10/25/2016...

Page Size 10 | Page 1 of 3320

Save Search as Default | Reset Default Search | Add | Edit | Select | Cancel

☐ 14

Highlight the record that you want to link (change or incident) and click “Select”.
The screen shot is an example of linking a change request to an incident record



where Service Request | ervice Request ID | Equal to | 41731 | Search

Request ID	Status	Customer	Owner Team	Owner	Subject	Created On
41731	Active	RT17986 - Torres, Rudy	Windows/AD	Magness, D...	Nexpose scans needed for servers	10/25/2016...
41730	Active	JC05699 - Anthony, Mark	Workstation...	Lawler, Walter	1 Dell 23" monitor for Mary Gomez	10/25/2016...
41729	Active	AD08306 - DelaGarza, Arturo	Workstation...	Lawler, Walter	1 Dell 23" monitor for Cynthia Barbosa	10/25/2016...
41727	Fulfilled		Identity and...	Wilkinson, K...	NTFS Request	10/25/2016...
41726	Active	AH09563 - Hernandez, Aurelia	Workstation...	Shepard-Hill...	SOFTWARE-Adobe Acrobat 8 Stand...	10/25/2016...
41725	Active	RK08329 - Korenek, Royce	Telecommu...		Extension Switch at Rosenberg High...	10/25/2016...
41724	Active	JL07139 - Luce, Jessica	Workstation...	Parker, James	INSTALL-1 Lenovo Think pad for Joe...	10/25/2016...
41723	Submitted		Cyber Security		CSFR - Cyber Security Firewall Requ...	10/25/2016...

Page Size 10 | Page 1 of 3320

Save Search as Default | Reset Default Search | Add | Edit | Select | Cancel

See CM-051 CR and Incident Linking for more information

CCB CHECKLIST

NOTE:

We encourage all areas of the business to have representation at the CCB. Your attendance is immensely important in helping us achieve our goal of only allowing the best changes into our production environment, thus preventing many unforeseen impacts.

Before the CCB Meeting

	Activity Needed - Outcome	***Detailed Steps to Complete***
□	1. If you are a recipient of the Planned Change Report	Review all items on the report and schedule for potential concerns or issues. If no issues or concerns are identified complete the A.C.T.I.O.N items.
□	2. For Standard CRs with a Planned status - Schedule QA/Techincal reviews	Attend QA or Technical review meetings. If a change request has an issue which cannot be resolved the change request status should be set to ***Draft***.
□	3. Maintenance CRs	For **Maintenance** change requests . • Ensure that the change request is thorough and complete (Contain the **A.C.T.I.O.N artifacts**) prior to the submission deadline. • Ensure that the status is Ready for Review. The submission deadline may be adjusted by Change Management as needed to accommodate holidays and other non-standard schedules. Maintenance CRs are due by Tuesday by 2:30PM. See CM-000 Change Management Policy and Procedures Roles and Responsibilities section page 8
□	4. For CRs with a Planned status - Ensure Change Request **Artifacts** are attached.	Change request should include, when applicable, but are not limited to the following: □ **A**ttach all IT Manager/Business approval (s) listed on the CR □ **C**yber scans need to be attached (when required) □ **T**est results need to be attached (If you can't please specify why) □ **I** Implementation, validation and rollback plans □ **O**peration manuals or support guide (as needed) □ **N**otification to users (if the change has downtime or user impact) □ additional documentation □ code or peer review □ release notes See CM-000 Change Management Policy and Procedures Roles and Responsibilities section page 8
□	5. Ensure your change requests are submitted with the status that applies for the change request type.	Status should be set to ***Ready for Review*** to be included on the CCB agenda.
□	6. If you missed the deadline	Your change will be targeted for the following CCB meeting.
□	7. Review Change Requests on the CCB Agenda	Review all change requests for potential impact to your area.

CCB MEETING CHECKLIST

Day of the CCB Meeting

	Activity Needed - Outcome	***Detailed Steps to Complete***
□	1. Attending CCB Meeting Wednesday at 9:00AM NOTE: Contact GRP_IT_ITSM if you do not have the CCB Meeting invite and they will forward it to you. When logging in via WebEx enter your first and last name. When calling in please announce yourself	**CCB Meeting Participation** CCB member participation includes voting on each CR on the agenda. **Attend in person** Conference Room G4A **Via phone** Call-in number: 1-240-454-0879 (US) Conference Code: 929 155 595 **Via WebEx** Join WebEx meeting Meeting Number: 929 155 595 Meeting Password: DPSITCCB
□	2. Presenting the Change Request at CCB	The Change Request initiator is responsible for presenting the CR for approval to the CCB members or identifying another individual to present the change. If the initiator/requestor is not the technical expert or the implementer, then the technical expert or implementer should be available to address questions that arise during CCB. **NOTE**: The Change Request will be placed on **Hold** if it is not presented during CCB.
□	3. If your Change Request is approved	Implement the change according to the Implementation plan

IMPLEMENTATION CHECKLIST

POST CCB Meeting

	Activity Needed - Outcome	*Detailed Steps to Complete*
☐	1. If your Change Request was not approved during CCB	Correct any issues that may have arisen during CCB and send an email to the Change Management team at GRP_IT_ITSM regarding completion of any pending approval items. If you do not complete this step your Change Request will need to go back to CCB for approval at the next CCB meeting.
☐	2. Making changes to an approved Change Request	Contact Change Management team at GRP_IT_ITSM regarding any changes to the Change Request. See CM-040 ITSM Changing Approved CRs
☐	3. Implement Change **NOTE**: Change should NOT start before scheduled start date/time. If there is a need to start early or if the CR requires any changes you will need to go through the Change Management group. Send an email to GRP_IT_ITSM to request a schedule change.	Follow the implementation plan submitted in the Change Request. **NOTE**: Please remember to contact OIC prior to starting the change and upon completion of the change. OIC: 512-424-2139 select option 3
☐	4. Closing a Change Request	**How to Close a CR** a- Attach pending artifacts (screenshots, validation results) **b-** If your CR in "**In Progress**" change status to one of these statuses 1- Rollback – requires a PIR 2- Implemented with Issue – requires a PIR 3- Successful implementation 4- Partial Implementation – requires a PIR c- Click on **Save** For information on completing a Post Implementation Review (PIR) **CM-052 Post Implementation Process** **NOTE**: The CR cannot be closed if OIC has not ended the change.

CM-000 Change Management Policies and Procedures

Information Technology Service Management

Document Version Date:
June 13, 2017

Revision 7.6.3

TABLE OF CONTENTS

Purpose

This document contains the change management policies and procedures that are outlined in the General Manual, Chapter 26.30 and that apply to all Texas Department of Public Safety (DPS) Information Technology (IT) production systems on or off premise. The change management process must be followed by anyone making changes to the IT production environment, including all DPS employees, contractors, and vendors. Managing change significantly increases system uptime and reduces outages and service interruption. With ever-growing demand and reliance on both DPS applications and infrastructure, it is critical that everyone follows the change management process and policies outlined in this document.

References

General Manual

CM-019 CR Review Process

CM_32_CR Emergency Approval

CM-040 ITSM Changing Approved CRs

CM-051 Linking Incidents to Change

CM-052 Post Implementation Process

Change Management at DPS

According to the DPS General Manual, Chapter 26.30,

Change management is the process of controlling modifications to hardware, networks, software, firmware, and documentation to ensure that information resources are protected against improper modification before, during, and after system implementation.

> The purpose of the Department's "Change Management Policy" is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. This applies to any and all DPS production systems regardless of where the system/solution is housed. Therefore, cloud hosted, vendor hosted, SAAS, etc. must also fully adhere these rules.
>
> The following are ways that a production system may be impacted without regard to the location, (HQ or DPS field office), or type of change, data or transactions, or level of impact, (low, medium or high), or who is responsible for maintaining the system, whether it be DPS

maintained, vendor maintained, or maintained by a third party: Implementation of new capabilities (system/solution)

- Deployment of a new solution
- Enhancing existing capabilities (system/solution/equipment)
- Interruption of service(s)
- Removal of existing capabilities
- Deployment of equipment (workstations, fingerprint scanners, cameras, routers/switches and related cabling and ports which have the potential of impacting ACL/VLANS or VPN tunnels)

All files, entities, system software, operating systems, linkers, compilers, PC-driven software and/or third party software are subject to change management control. Examples include, but are not limited to changes to, cloud solutions, source files, configuration files, scripts, tables, Oracle, DB2, SQL, UNIX, Linux scripts, software development tools, and any files required to generate builds or reproduce a system (hardware, firmware, operating system, and software). Infrastructure (i.e. network, active directory, and password) changes that have the potential to impact any of the hardware that is supporting the DPS IT systems are also subject to the change management process. Change is inevitable and necessary in an IT environment, and DPS is no exception. The agency's change management policies and procedures do not prohibit changes that are necessary to improve and protect DPS systems. Rather, they enforce managed change in order to communicate changes and minimize impact to the business, law enforcement, and most importantly, the citizens of Texas.

Objectives

Using the change management process ensures that changes to DPS off or on premise systems are properly documented, reviewed, authorized, communicated, verified, tracked, and implemented with minimal disruption to service levels. The change management objectives include:

- Using standard methods, policies, and procedures to support the prompt handling of all change requests (CRs).

- Providing the information and the review/authorization process necessary to affect Change Control Board (CCB) and management decisions regarding CRs. This process ensures CR reviews and authorizations are consistent.
  Note: The process is shortened to adjust to business needs during a crisis.
- Staging and testing the release by the Release Management team if applicable.
- Reviewing and authorizing at the weekly CCB meeting with any pending deficiencies noted.
  Note: The approval process varies for FYI and Emergency CRs. See the section **Change Request Types** for more information.
- Promoting open communication and awareness among all parties.
- Eliminating any two or more conflicting changes from occurring.
- Requiring that the OIC be phoned when the change starts, pauses, resumes, or completes.
- Requiring that the CR be closed within one business day with the correct status and comments to communicate success and/or identify issues.
- Ensuring changes maintain or improve system stability and protect the integrity of IT resources including files and data.
- Identifying the level of risk that changes pose to IT production systems.
- Schedule compatible CRs to reduce the possibility of outages.
- Ensuring accountability, repeatability, and transparency.
- Maintaining a database that contains current and historical CR information.

Complying with DPS IT Change Management

Failure to comply with the DPS IT Change Management Policies and Procedures may result in the following disciplinary actions per the General Manual:

- “It is the supervisor’s responsibility to counsel an employee whenever the employee’s performance slips below the ‘Acceptable Performance’ level.” (General Manual, Chapter 07.62.09.2) This may be in the form of informal or verbal counseling to address any initial issues.

- Formal counseling may be employed if the initial informal counseling does not sufficiently correct the employee's behavior. Per the General Manual, Chapter 07.62.09.2.a,

> 3) The supervisor will document the counseling using an HR-31 Counseling Record. The counseling document is to be signed by both the supervisor and employee. The supervisor will provide a copy to the employee and keep the original in the employee's local file.
>
> 4) If the employee's performance does not improve to the "Competent" level within the established time frame for improvement, the supervisor will develop and administer a Performance Improvement Plan (PIP) for the employee (see next paragraph). This potential PIP consequence should be cited on the counseling document as fair warning to the employee.

- Should habitual failure to comply with the DPS IT Change Management Policies and Procedures continue after informal and formal counseling, then per the General Manual, Chapter 06.30.00.02,

> Any of the major infractions listed as follows may be deemed sufficient cause for the discharge, suspension, demotion, or removal of any member of the Department of Public Safety:
>
>> 3. Violation of any rule, order, requirement, or failure to follow instructions contained in Department manuals;
>>
>> 5. Willful neglect of duty;
>>
>> 10. Willful or inexcusable destruction or loss of state property;
>>
>> 13. Any act on or off duty which reflects discredit to the Department of Public Safety.

Roles and Responsibilities (see General Manual 26.30.02 – 3, 5, 6, 8)

Change management requires coordination and communication among IT, customers, and vendors that are involved with changes to DPS IT on or off premise production systems. To maintain an effective change management process, full cooperation between individuals and teams responsible for requesting, implementing, validating, and approving change requests is required, as is clear communication between all affected groups, including the ITSM team.

Change Control Board (CCB) Attendees

Refer to the section **Change Control Board**.

Emergency CCB Distribution List Members

Refer to the section **Change Request Types>Emergency**.

Initiators/Requestors

The initiator/requestor is the individual who opens the change request and is responsible for it through its lifecycle (creation, coordination, implementation, tracking, validation, and closing). The initiator should always be the individual most familiar with the change and capable of monitoring, tracking, and answering questions about it. Typically, this should be the individual or a member of the team implementing the change. Initiator responsibilities include, but are not limited to the following:

- Following all the procedures in this manual regarding creating, implementing, and closing CRs
- Ensuring that all planned change requests have been submitted by noon on Friday (required for Standard CRs only)

Note: If the Friday deadline is missed and the change needs to be implemented prior to the next CCB, either the FYI or ECR process can be used to process a change request. The criteria for FYI or ECR need to be met. See Change Request Types section for information.

- Ensuring that QA or Technical review meetings are held prior to noon on Tuesday
- Change request form can be modified when the status equals “Planned” and CCB decision field is blank or equals “In CM Review Pending Update”
- Ensuring that the change request is thorough and complete prior to the submission deadline of 2:30 PM (HQ Time) on the day prior to CCB. The submission deadline may be adjusted by Change Management as needed to accommodate holidays and other non-standard schedules

Important: CR's that are not complete will **not** be included in the Agenda for CCB review without DAD authorization.

- Obtain necessary approvals, including customer(s), IT manager(s), implementer manager(s), etc.

- Collect and include the necessary information and completed documentation (test results, QA sign off, release notes, etc.) from all affected parties or groups performing, testing, or who are otherwise part of the change

- Ensure that changes have undergone a code and/or peer review. Code/Peer review question should always be answered. Appropriate responses are Yes, No and NA. A Yes response will enable the Code/Peer reviewer name field. Complete this field with the name of the person who reviewed the change. This normally should not be the same person as the implementer.

    - Code Review

        - Ensure that any code and scripts have been reviewed and approved by another individual knowledgeable in the area that the change relates to;

        - Ensure that all code and scripts have been stored in an approved version control management system (i.e. SVN) and provide link to the specific tag in the repository, or, if stored in the trunk, indicate the revision number;

        - If an SVN repository is unavailable, store items in a network location accessible to Change Management staff. If there is no other location available, items may be attached to the Change Request, however they should be stored in a format that will not allow accidental execution, i.e. SQL scripts should be stored as.txt.

    - Peer Review

        - Ensure that all plans (implementation, rollback, and validation) and schedules related to the change have been reviewed and approved by another individual knowledgeable in the area that the change relates to.

- Coordinate with and ensure all necessary staff and resources will be available for the proposed change

- Include the schedule (CRs spanning multiple days)

- Submitting complete (may include but not limited to: test results, email approvals from all of the IT and Business Managers listed on the change request form, operation manuals for new or changes to user facing services) CRs in Ready to Review status before the CCB submission deadline.
  Note: The ITSM team will return a CR to Draft status if it is incomplete and not ready for presentation at CCB. This could result in the CR not going to CCB.

- Presenting the CR for approval to the CCB or identifying another individual to present the change. If the initiator/requestor is not the technical expert or the implementer, then the technical expert or implementer should be available to address questions that arise during CCB.
  Note: If no one in attendance can effectively present the CR, it will either be returned to Draft or be placed in CCB Hold and will **not** be approved. It must be presented for approval at the next CCB.

- Coordinating with all groups, including IT, business users, contractors, and other non-IT or non-DPS entities involved with the change.

- Keeping ongoing CRs up to date and notifying necessary parties of any changes.

- Notifying the ITSM team and the OIC of any schedule changes, extensions, or cancellations that will affect the time or duration of a change, however, only ITSM has the authority to approve extensions or schedule changes.

For a complete list of submissions requirements, see **Standard Change Request Process**.

Implementers

Implementers are the individuals performing the work outlined in the change request. Their responsibilities could include, but are not limited to, the following:

- Calling the OIC before starting the change and again after completing the change

- Verifying that the change(s) that they performed were successful

- Capturing validation artifacts when applicable

- Coordinating and communicating with anyone else involved with the change

- Documenting any problems or issues that arise during implementation

IT Managers

The IT group(s) performing changes and their managers are accountable for the technical success or failure of a change. Thus, IT managers are expected to ensure the following:

- Their staff follows Change Management procedures
- They are aware of their staff's changes
- Their staff enters and submits complete and accurate CRs
- Changes are justified and approved by all necessary parties

  Note: All Change Requests require both an IT and Business Approver. The IT and Business Approver cannot be the same person. In the event there is no Business Owner, the IT Team Lead or higher can be the Business Approver. In this case, the IT Approver must be that individual's supervisor or above.

- Potential impact has been identified and evaluated
- The changes in the CR are tested to the highest degree possible prior to implementation
- Implementation, validation, and rollback plans are documented in the appropriate location on the CR or are attached to the CR
- Support from other IT groups, the business, and vendors are committed for applicable changes
- Necessary communication, documentation, training, procedures, and announcements are completed and distributed to all affected groups
- The correct resources are available to implement the change on time
- The correct people attend the CCB meeting

Executive Management

The DPS CIO, Deputy CIO, and Deputy Assistant Directors (DADs) will resolve any issues that are escalated to them and have veto power over all change requests.
Note: Unless otherwise determined, escalation should follow the chain of command.

Non-IT Entities

All DPS IT staff is subject to and accountable for the Change Management process, as are DPS non-IT departments, and external entities that are involved with changes to DPS IT on or off premise production systems. DPS IT staff is responsible for proper communication and coordination with non-DPS IT groups to ensure that those groups are aware of and follow the CM process.

Change Control Board (see General Manual 26.30.02 – 3, 6)

The Change Control Board (CCB) and Emergency CCB are the bodies that approve or deny changes. For information on the Emergency CCB, see **Change Request Types>Emergency**.

Attending

The CCB is comprised of the individuals in attendance at each week's meeting. We encourage all areas of the business to have representation at the CCB. Your attendance is immensely important in helping us achieve our goal of only allowing the best changes into our production environment, thus preventing many unforeseen impacts.

Attendees must always include the following:

- Staff who represent all areas of IT (infrastructure, operations, applications, governance, and information security).
- Division representatives (business customers).
- Additional personnel aware of or with an interest in the changes on the agenda.

The CCB meets every Wednesday with exceptions during holidays; the Change Management team will send notifications for cancelled or rescheduled meetings. The Outlook calendar invitation and agenda emails contain the conference room locations, conference bridge information, and WebEx meeting information. The agendas and release schedules themselves also contain the conference bridge and WebEx details.

The Change Management team emails (and posts to SharePoint) the agenda the day prior to the CCB meeting and the release schedule and minutes the day of the meeting: http://portal/sites/it/operations/itsm/CCB/Forms/Newest%20First.aspx. CCB meetings are also recorded via WebEx and available on the SharePoint site after the minutes have been distributed.

The Change Management team sends meeting invitations, agendas, release schedules, notes, and other change-related communications to the GRP_ChangeManagement@dps.texas.gov distribution list. Any DPS employee interested in attending or taking part in CCB meetings should contact their Local Security Administrators (LSAs) to request addition to the list. Emergency CR approval notifications are sent only to the grp_it_Emergency_CCB@dps.texas.gov distribution list.

Responsibilities

CCB attendees assume the following responsibilities:

- Review and become familiar with the agenda prior to the meeting.
- Bring any questions about CRs that are on the agenda to the meeting.
- Use good meeting etiquette.
    - Pay attention to those speaking, stay engaged, and do not hold side conversations.
    - Be punctual, both when attending in person or via teleconference/WebEx.
    - Stay on topic. If additional or tangential discussion is needed, it should be taken offline.
    - Speak clearly and loud enough to be heard. If in a conference room, stand near a microphone.
    - Enter their names when joining the meeting via WebEx for accurate attendance records.
- Conference bridge connections may be muted by the organizer in these situations:
    - Excessive noise or static is present. Bridge attendees should mute their phones when not speaking.
    - An attendee places the conference call on hold.
- Review the release schedule and meeting notes after the meeting and send any corrections to the Change Management team.

Approvals

The CCB reviews and makes decisions on Standard and Maintenance CRs. The Change Management team has been delegated the authority to approve FYI CRs on behalf of the CCB, and Emergency CRs follow their own approval process. For additional information on the CR types, refer to the section **Change Request Types.**

All changes presented to the CCB must receive unanimous approval to move forward. Each attendee has veto power, so it is extremely important that everyone reviews the agenda before the meeting. Executive management may assume responsibility and override a veto if they deem the change necessary and the risk acceptable.

The CCB makes one of four decisions on changes.

- **Approved** – The CCB approves the CR in its current form, authorizing the change to occur.
- **To Be Determined (TBD)** – Change Requests in TBD status have not yet been approved for implementation. The CCB grants conditional approval. The individuals responsible for these CRs must contact the Change Management team before moving forward so the CR can be reviewed and the CCB decision updated to Approved. If the issue that caused the CR to be placed in TBD status is not resolved prior to the CR's scheduled start date/time, the Change Request will be placed back into Draft status and will need to be rescheduled and resubmitted for CCB Approval TBD will not be used for incomplete change request prerequisites:
  - **A** – Attach approvals (for all IT Managers and Business Owners listed on the CR)
  - **C** – Cyber scans (when required)
  - **T** – Test results (If you can't please specify why)
  - **I** – Implementation, validation, rollback plans
  - **O** – Operation manuals or support guide (as needed)
  - **N** – Notification to users (if the change has downtime or user impact)
- **CCB Hold** – The CCB does not consider or render a decision on the CR; it can be resubmitted at a subsequent CCB. A hold typically occurs because no one attends to present the change.
- **Denied** – The CCB or Emergency CCB denies the CR. It must be returned to Draft status and resubmitted at a later date, or it must be cancelled. Though extremely rare, this decision may result if members of the CCB have objections to the change that cannot be resolved, either during the meeting or in offline discussions.

Note: If the change is not complete or ready to move forward, it will be returned to Draft status and will not be considered. The CR may remain open and be resubmitted for consideration at a subsequent CCB.

If a change is questioned after it has been approved by the CCB, Change Management will;

- Change the Change Control Decision to "TBD"
- Notify the Initiator and IT Manager

- Initiator and or IT Manager will be responsible for resolving the concerns prior to the CR's scheduled start date/time.

The CR will be placed back into Draft status and will need to be rescheduled and resubmitted for CCB approval if the issues are not resolved prior to the CR scheduled start/end time.

Emergency CCB

The Emergency CCB is a comprised only of IT management and other key IT stakeholders. These individuals are responsible for reviewing and responding to the Emergency Change Approval Request email with approve, disapprove or NA in a timely manner. All Emergency CCB members are part of the GRP_IT_Emergency_CCB distribution list. Refer to the section **Change Request Types>Emergency** for further information on Emergency CRs.

Change Request Processing Rules (see General Manual 26.30.02 – 4, 12)

Before changes to DPS IT on or off premise production systems, deployment of any new system/solution, and/or deployment of equipment, cameras, routers/switches either in HQ or DPS field offices (project related workstations and finger print scanners), may be performed, change requests (CRs) must be presented to and approved by the Change Control Board (CCB), or the Change Management team as authorized by the CCB. As of publication of this document, CR forms are maintained in the Change Management System. To determine which CR type to use, refer to the section **Change Request Types**.

For more information regarding the CR Review Process, see CM-019 – CR Review Process.

Planned Submission Deadline

All **Standard** type CRs should be submitted with a status of ***Planned.*** All planned standard CRs will be reported on in the DPS – Planned Change Report and sent every Friday at 2:00pm. Recipients of the report will have an opportunity to review the items on the agenda and schedule meetings as needed. When ready, the CR should be completely filled out including the A.C.T.I.O.N items and status should be changed to ***Ready for Review***.

The Planned status process is not applicable to FYI and Maintenance CRs. The status should be set to ***Ready for Review*** for FYI and Maintenance change requests.

Ready for Review Submission Deadline

To be presented at the CCB meeting, all Standard and Maintenance CRs with planned start times between Wednesday (day of CCB) at 10 am through the following Wednesday at 9:59 am, must be **complete** and submitted in Ready to Review status by **2:30 PM (HQ time) on the day prior to the CCB**. This allows the Change Management team time to perform a final review prior to distributing the agenda to CCB members that afternoon.
Note: The deadline will change as needed due to holidays, closures, rescheduled meetings, etc.

CRs must be in Ready to Review status to be reviewed and included on the CCB agenda. Those in Draft status are not reviewed and will not appear on the agenda. To submit a Change Request after the deadline, the implementer, initiator, or someone who can speak about the change must contact the Executive Management team to explain their change and its urgency. Executive Management will ultimately decide if a Change Request will be permitted, or if it must wait until the next appointed CCB.

Scheduling

When determining the planned start and end of a change, consider the impact that performing the change will have on the business and other IT areas. Account for complexity, location, if other teams or if vendors are involved, etc. It is better to estimate a longer implementation and validation period and finish early than require more time than originally planned for.

Avoid scheduling changes to occur during critical processing periods as defined by the business. If a change is necessary during these periods, escalation to an appropriate impact level should be considered based on the potential for interruption of processing.
Note: Refer to the section **Change Request Risk Assessment** for additional information about impact levels. Some examples of critical processing periods can include, but are not limited to:

- Month-end close/processing according to the production schedule.
- Year-end close/processing according to the production schedule.
- Prime processing period: Monday through Friday, 7 am-6 pm Central.
- During periods when there is a high potential for urgent or emergency situations (e.g., inclement weather).
- High traffic periods (see CCB Change Freeze below).

Change Freeze

Change Management places a "freeze" on our production environment based on the published Change Freeze Schedule and emergency change freezes. Production changes should not be made during this time. This ensures that our production environment is in a stable condition during periods of increased risk.

What is a freeze?

Change freezes are based upon potential risk and resource availability. Therefore,   Change Freezes are routinely set to occur during times of high-profile situations, possibly affecting public safety, to ensure all systems remain at 100% stability and availability. Change Freezes also occur to ensure proper resource levels are available to assist in recovery, if issues are encountered.

There are two types of freezes:

- **FULL CHANGE FREEZE:** This means that no standard changes are approved to be implemented during this timeframe.
- **LAW-ENFORCEMENT CHANGE FREEZE:** This means that no standard changes affecting or having the potential to affect any Law-Enforcement system are approved to be implemented during this timeframe.

  The Texas Department of Public Safety (DPS) increases patrols for an eight-day period that includes both the Christmas and New Year holidays. From **Dec. 24 – 27 and Dec. 31 – Jan. 3, DPS troopers**, as well as law enforcement across the state, increase patrolling roadways throughout the holiday weekends looking for drunk drivers, speeders, seat belt violators and other drivers who are endangering themselves and others.

  NOTE: See DPS New Press release https://dpsnet/Divisions/DirectorStaff/PIO/index.htm#press

Freeze Specific Information

What prompts a change freeze?

- Specific holidays see the Change Freeze schedule for details
- Regularly scheduled community events (ROT, ACL, Formula One Racing etc.) that can increase of the need for critical Law Enforcement related systems
- Unscheduled events that are requested by agency divisions or external Law Enforcement partners
- Emergencies caused by nature, manmade disaster or other events

What is the impact of a Change Freeze on the Department?

- No changes are to be made to the production environment
- Freezes are comprised of the duration of the event

What are the exceptions during a change freeze?

The following changes will be reviewed and may be approved by Change Management during the change freeze:

Full Change Freeze - Exceptions

- Emergency Change Requests as defined in CM-000 Change Management Policies and Procedures
- Other changes that executive management has authorized and deemed necessary

Law-Enforcement Related Change Freeze - Exceptions

- Emergency Change Requests as defined in CM-000 Change Management Policies and Procedures
- Other changes that executive management has authorized and deemed necessary
- Changes to systems that do not affect law enforcement's ability to conduct business

What communication needs to go out prior to a freeze?

- A member of the ITSM team will do the following:
- Post the change freeze schedule on the ITSM SharePoint site annually and post new change freeze dates as they are approved
- Send written notification to OIC and the Change Management D-list
- Announce at CCB

What is the procedure to request a change freeze?

Send request to GRP_IT_ITSM with "Change Freeze Request" in the subject line of the email. Requests should be submitted by management

The request should contain the following items:

- Description and Justification
- Start and end dates
- Type of Freeze: full or LE
- Approving requesting manager

Request will be processed by Change Management

Requirements

All change requests must include at least the following details before they are submitted for approval or inclusion on the CCB agenda.

- **Implementation plan** – What work is being performed, by whom (when more than one implementer), communication hand-offs

- **Validation plan** – What actions will be taken to verify that the change completed successfully in production.

- **Rollback plan** – What work will be performed if problems arise during or resulting from implementation? The plan gives the implementer the ability to restore business continuity quickly.

- **Test results** – Whenever non-production environments exist, testing prior to implementation is required, and those results must be attached to the CR or included in the details. Where QA is involved, QA must sign off on all testing. They will attach their approvals to the change requests.
  Note: If results cannot be captured or testing is not possible ("pure production" change), validation results must be captured after implementation and included in or attached to the CR when possible.

- **Approvals** – The Business Owner Approval, the IT managers of the affected areas, and the managers of the implementers (if other than the affected areas) must approve the CR. Approval emails are required for all Business Owner and IT Managers listed on the change request and must be attached to the change request.
  Note: Assignment of work orders does not constitute manager or customer approval for the CR. All Change Requests require both an IT and Business Approver. See Change Request Types for approval requirements for maintenance change requests. The IT and Business Approver cannot be the same person. The person implementing the change cannot be the business approver. In the event there is no Business Owner, the IT Team Lead or higher can be the Business Approver. In this case, the IT Approver must be that individual's supervisor or above.

- **Implementer** – The implementer(s) should be the individual(s) who will be performing the work. Implementer(s) outside of the IT Approver's team must have their Manager's approval to be an implementer. The IT Manager's name must be listed on the change request form and email approval must be attached.

Note: Assignment of work orders to individuals does not constitute contacting them to check availability for the implementation, nor does it indicate manager or customer approval for the CR.

- **CR Required Fields** – All required fields are designated by an asterisk and may vary based upon responses to other questions.
- **CR Required Content –** Additional details that must be included (script names, database names, server names, IP addresses, list of affected machines, SVN repository, etc.) vary based on the change and associated work being performed.

Rolling/Ongoing CRs

Rolling or ongoing CRs are an exception. A change request that encompasses a project will be entertained at CCB on a case-by-case basis. The area submitting the CR must keep it updated and current for the duration of change. This is essential for any CR that has a rolling schedule, especially one with work occurring across multiple areas, days, locations, and/or tasks.
Note: If the CR is not maintained and updated regularly, the CR may be closed and the affected area will be required to submit separate CRs for future work that is related to the project.

Maintaining CRs

To effectively manage and monitor changes, CRs must be kept accurate and current. The initiator, assignee, or implementer is responsible for ensuring any necessary details are added to or included in the CR.

Changing Approved CRs

Once a CR is approved, either by the CCB or by the Change Management team as authorized by the CCB, no changes should be made to it before implementation except in the following situations.

See **CM-040 ITSM Changing Approved CRs** for additional information.

Schedule Changes

When unforeseen issues arise, planned start and planned end times may be rescheduled for change requests that have been approved but have not yet begun. In those cases, the initiator, assignee, or implementer is responsible for acquiring approval from the customers and IT managers and for seeking approval from the Change Management team (GRP_IT_ITSM@dps.texas.gov) who will verify that there are no conflicts with pre-existing CRs. Once the new schedule is approved, the Change Management team will notify the OIC and other appropriate parties of the change.

Note: If the rescheduled time falls within the next CCB cycle, the CR may need to be presented again.

If the change has already begun, only the planned end may be updated; the planned start may not be modified. Customers and managers must still approve, and Change Management must approve, update the CR, and notify the OIC and other appropriate parties as needed of the new schedule.

Cancelling

If no work associated with the CR has occurred, and the clock has not yet started, approved CRs can be cancelled. The CR can also be returned to Draft status and resubmitted to CCB at a later date if the work is still expected to occur. In those cases, notify the Change Management team so the CCB decision can be updated.

If any work has occurred, the CR cannot be cancelled. It must be closed as rolled back, partially implemented, or implemented with issues; depending on how much of the implementation was performed.

Altering Implementation Details

Once a CR has been approved, no implementation details should be modified or changed. If something in the implementation plan, validation plan, or possibly the rollback plan needs to be updated, contact the Change Management team. They will assist with determining if the details can be altered or if a new CR is required.
Note: If it is discovered after approval that other individuals or teams are needed, then the individuals and their managers must be notified prior to the start of the change to ensure that they are available. If not, the change may need to be rescheduled.

Closing

Change requests may remain open for up to one business day after completion. The initiator, assignee, or individuals implementing the change are responsible for updating the closing notes, adding any additional information or documentation that is required (e.g., post-implementation Results (PIR), validation artifacts), and closing the CR.   For more information on the PIR process read **CM-052 Post Implementation Process**.

Note: The Change Management team will follow up on change requests that remain open past the one business day grace period.

Reopening

No one outside the ITSM team is able to reopen a closed CR. If the team determines that the CR does need to be reopened, then they will address the issue at that time. Contact the ITSM team (GRP_IT_ITSM@dps.texas.gov) if a closed CR needs to be modified.

Cancelled and closed change requests may not be reused. If an issue arises from a closed CR, a new one must be created and the previous CR identified in the new one.
Note: If needed, use the copy functionality in the Change Management System to create a similar CR.

Production Pilots

For information about production pilots, refer to the **CM-031_Pilot_Change_Requests_and_Release_Management** document on the ITSM SharePoint site: http://portal/sites/it/governance/itsm/documents/Documents/.

Unauthorized Changes

An unauthorized change is a change made to a DPS system for which a change request (CR) should have been submitted and approved but was not. If a CR does not already exist for the change, the individual or team that performed the change must create and submit a CR for review. Unauthorized changes must contain the same information as any other CR; the requirements are no different.
Note: If ever unsure if work requires a change request, contact the Change Management team (GRP_IT_ITSM@dps.texas.gov).

Change Request Types (see General Manual 26.30.02 – 4, 8, 9, 10)

Change requests (CRs) may be submitted as one of four types: Standard, Maintenance, Emergency, or FYI. All CRs, regardless of type, must be thorough, complete, and follow the Change Management process. Refer to section **Change Request Processing Rules** for requirements.

The primary differences between CR types are impacts and approval processes. As part of the review, the Change Management team may determine that a change request qualifies as another type and will work with the initiator accordingly to ensure that the CR is processed correctly.

Standard

Standard change requests follow the default Change Management process (see the section **Standard Change Request Process**). This means that these changes must be presented to and approved by the Change Control Board (CCB) at the weekly meeting prior to implementation. The goal should always be to submit a change as a Standard CR and take it to CCB for approval. Standard change requests must be complete, have test results, user notification, IT and Business approvals emails, support instructions or manuals and cyber scan report (as needed) attached to the CR prior to submitting for approval. If a CR is missing any of the required documentation will be set back to DRAFT and will need to be reviewed at the next CCB.

Maintenance

Maintenance change requests are for routine maintenance that occurs on a regularly scheduled timeframe and have business owner and IT manager approval. Maintenance CRs follow the **Standard Change Request Process**. However, even though Maintenance CRs are announced during the CCB meeting, unless someone has a specific question about them, they do not require representation and discussion and will be approved.

Before a change can be submitted as a Maintenance CR, it must first be presented as a Standard CR to the CCB. The implementer/team must have already demonstrated that well-documented processes are available and are being followed via previous changes and notified the CR approvers that a request will be submitted to reclassify the Standard CR to a Maintenance CR. The approval of the Standard CR will serve as the approval for all further Maintenance CRs. The individual presenting the change can request that it be considered maintenance. Once approved by the CCB, the change can be submitted as a Maintenance CR in the future. CRs approved to be Maintenance include the following:

- FAST DISPO TLE Servers: Microsoft updates/restart (e.g., 9949) – CCB approved 04/20/2011
- Weekly NEC AFIS server maintenance (e.g., 9950) – CCB approved 04/20/2011
- AFIS CBM basic weekly maintenance (e.g., 9910) – CCB approved 04/20/2011
- AFIS quarterly cold backup and weekly server maintenance (e.g., 9908) – CCB approved 04/20/2011
- Apply [Month Year] Security Updates to SCCM servers (e.g., 9930) – CCB approved May 2011
- Windows Server Critical & Security Updates - Ongoing Maintenance (e.g., 9884) – CCB approved April 2012
- Windows Updates for Blackberry Servers (e.g., 9525) – CCB approved 04/24/2013

- Update Windows 7 x32 and x64 Workstation images with current patches (e.g., 10117) – CCB approved 10/16/2013
- MorphoTrust-Apply MS and SQL patches to IVS Servers (e.g. 2964) – CCB approved 6/10/2015
- Excess equipment and power cord cleanup (e.g. 3698) – CCB approved on 10/7/2015
- Quarterly III SYNC (e.g. 5098) approved on 0/12/2016
- Apply Windows CSA updates on the IVS system and reboot. CCB approved on 10/26/2016
- Planview Schedule Maintenance (e.g. 6205) approved on 1/25/2017

Note: If habitual issues arise from a Maintenance CR, it may be removed from the approved list and must be submitted as a Standard CR until stability is demonstrated.

Emergency

Emergency change requests are submitted when the production environment is being, or is in danger of being, impacted by a situation that needs to be addressed immediately. Emergency CRs are time sensitive and typically high impact. Because they cannot wait for a CCB meeting, they must instead receive approval via voting email by the Emergency CCB members. It is the responsibility of the Emergency CCB members to carefully review the Emergency notification e-mail and notify users who may potentially be impacted by the change prior to approving the request.

Emergency change requests must include the approvals of the Manager and/or DAD of the area implementing the change or their delegate must have the business approval and test results attached to the ECR prior to submitting ECR for review/processing. The Emergency CCB members will receive an Emergency Change Approval Request email with the ECR details. They are responsible for reviewing and responding to the Emergency Change Approval Request email with approve, disapprove or NA. There is a two hour window for processing the change and allowing for disapprovals. If you do not approve the change, a response is required within the 2 hour window. Change Management will assume that you approve the change or the change does not impact your area of responsibility if a response is not received within the 2 hour window. In the event where a mission critical system is impacted, the allowed process time will be 30 minutes If an immediate change is needed call the OIC to establish an Emergency Call Bridge. If a negative response is received, the change will not receive final CM approval until the concern is resolved and that individual has provided approval.

At any time, Executive Management can opt to override this policy when a more expedient approval is needed for an exceptionally urgent request.

OIC Emergency Call Bridge

While rare, when situations warrant it, during the course of an emergency call bridge hosted by the OIC, it is determined that a change is needed to resolve a major issue, or outage and it must be done immediately, the attendees of the emergency bridge will become the Emergency CCB. The CM representative will ask if there are any objections to performing the change. If there are no objections, the CM representative will declare that change approved and will need to obtain a roll of all individuals on the call (this can usually be obtained from the OIC)—these names will represent the Emergency CCB for that change. The implementer must still complete an Emergency CR after the call concludes, however once CM reviews it and ensures it is complete, it will not have to be sent out for approval. The CR can be marked Approved and the list of individuals who represented the Emergency CCB should be attached to the CR. This is the only situation in which approval for an Emergency CR from the Regular Emergency CCB distribution list is not required. This will NOT be an unauthorized change.

Note: All Emergency CRs must follow the **Change Request Processing Rules** as well as contain the justification, regardless of whether the CR is submitted and approved prior to or after the change.

Emergency CRs should meet any of the following criteria:

- A production area is down (e.g., 9779).
- Critical systems are slow to respond, and the issue is impacting users (e.g., 9880).
- Critical information is being misprocessed (e.g., 9780).
- There is a security risk (e.g., 9804).

In some cases, Change Management will work with the customer, IT group, and/or management to determine if a change without one of these criteria should be processed as an Emergency CR. If there is an exception, it is typically to provide visibility of the impending change. Regardless of what the CR may involve or its impact, an IT Deputy Assistant Director (DAD) or other member of executive management can assume responsibility and deem a CR an emergency.

FYI

FYI change requests are primarily informational. FYI CRs are in place to allow IT and the business to perform changes that will have no, or very minimal, impact to production systems and the agency. The Change Management team reviews and approves FYI CRs. Approval notifications are sent to the OIC, the initiator, and the assignee.

FYI change requests must be complete, have test results, user notification, IT and Business approvals, support instructions or manuals and cyber scan report (as needed) attached to the CR prior to submitting for approval.

FYI CRs cannot result in an outage, downtime, or adversely impact the agency. Whether or not a change can be submitted as an FYI ultimately depends on the extent of the change and its possible impact. Examples of changes that may and may not be submitted as FYI CRs are included below.

The following list identifies examples of changes that **could** be submitted as FYI CRs, provided there is no or very low risk associated with them.

- Changes with no or minimal impact.
    - Adding disk space to a server with no service interruption.
    - Replacing a failed UPS where the outage is local and installed afterhours
    - Minor firewall configurations (e.g., CR 9923).
    - Adding/migrating SVN repositories (e.g., 9308).
    - Active Directory changes that do not cause an interruption of service (e.g., 9659).
    - Low- or no-risk configurations (e.g., CR 9890).
    - Equipment moves with no associated downtime (e.g., CR 9719).
    - Microsoft Exchange rules (e.g., CR 9918).
    - Remove domain controller role (e.g., 9735).
    - Create, remove, or update ticket templates used only by your team (e.g., 10045).
- Minimal or non-intrusive database changes.
    - Extend table space.
    - Creating indexes (e.g., 9751).
    - Add a value to a table (e.g., 8894).

- Minimal or non-intrusive application changes.
    - Revise JCL to run a report (e.g., 9889).
    - Revise email addresses embedded in JCL (e.g., 9620).
- Equipment decommissions (e.g., CR 9924).
- Post new or updated reports (e.g., Crystal Reports, HEAT).
  Note: These are only allowable if there are no associated database modifications.
- Changes to non-production systems (e.g., updates made to a development environment).

Not Allowed

Certain changes, regardless of impact or possible downtime, cannot be submitted as FYI CRs. These include but are not limited to the following:

- Production database structural or schema revisions (e.g., 9696).
- Requiring Alchemist promotion (e.g., 9874).
- Requiring Turnover promotion (e.g., 9844).
- Application code (e.g., 9920).
- MPLS conversions (e.g., 9708).
- Adding/swapping devices on the network (e.g., routers, servers, switches, phone systems).
- Server software/OS upgrades (e.g., 9929).
- Software patches (e.g., 9685).
- F5 configurations (e.g., 9916).
- System UI or functionality (e.g., 9902).
- Adding or removing vCPUs on virtual servers (e.g., 9917).
- Agency-wide Microsoft workstation updates (e.g., 9932).
- Agency-wide Sophos updates (e.g., 9561).
- Any FireAMP, AMP or StorageAMP changes
- Power-related Facilities work in a data center (e.g., 9729).
- Implementation of new on or off premise capabilities
- CRs already approved to be Maintenance CRs.

Note: Exceptions may be granted on a case-by-case basis.

Change Request Statuses

The status in which a change request (CR) has been placed indicates where the CR currently is in the workflow and is indicated by the **Status** field on the CR form.

Open Statuses

While a CR is open, it is important to ensure it is in the correct status:

- **Draft** – The default status upon CR creation indicates that the CR is incomplete and is not ready to be reviewed by the Change Management team.
  Note: The Change Management team does not monitor or track changes in Draft status.

- **Planned** – Standard CRs that are planned for implementation during the current release timeframe.

- **In Progress** – In Progress is set automatically once the OIC starts a CR.

- **On Hold** – The CR has been placed on hold by the initiator, assignee, OIC, and/or implementer. This is usually due to unexpected issues encountered prior to actual implementation. If the causes for the hold result in rescheduling, the Change Management team must be contacted first. Changes that span multiply days (aka rolling CRs), need to be placed on hold when work has been temporarily stopped. The CR implementer, assignee or requestor is responsible for contacting the OIC to pause the change. The process will set the CR status to hold.

- **Ready to Review** – The CR is ready for the Change Management team to review for completeness.

- **Rollback-Open** – The CR was rolled back but remains open for rework within one business day.
  Note: If the rework and corrections require more than one business day, the change should be closed and a new CR submitted when the change is ready to move forward.

Closed Statuses

When closing a CR, be sure to select the correct closing status.
Note: The Change Management team may reopen a closed CR and change the status if it is deemed necessary.

- **Cancelled** – No work has occurred, and the CR has been cancelled.
- **Implemented With Issue** – The change was implemented but with unexpected results. If issues were encountered during implementation, the CR should be closed in this status even if the change was ultimately successful. This status type requires a post implementation review (PIR) to be completed in the ITSM tool.
- **Partial Implementation** – Part, but not all, of the CR was implemented. This status type requires a post implementation review (PIR) to be completed in the ITSM tool.
- **Rollback** – The change was rolled back, and the system, application, or item to be changed has been reverted to its state prior to any work occurring. This status type requires a post implementation review (PIR) to be completed in the ITSM tool.
- **Successful Implementation** – The entire CR was completed successfully with no unforeseen challenges or issues.

Change Control Board Decisions

The decisions made by the CCB (see the section **Change Control Board**), Emergency CCB (see the section **Emergency Change Request Process**), or by the Change Management team as authorized by the CCB are reflected in the **Change Control Board Decision** field on the current change request (CR) form. A CR will always be assigned one of the following decisions:

- **Approved** – The CCB, Emergency CCB, or Change Management team has approved the CR in its current form, authorizing the change to occur.
- **Awaiting Approval** –The CR has not been reviewed and no decision has been made. **Note**: When a CR is moved back to Draft status, the decision is returned to Awaiting Approval.
- **Awaiting Emergency Approval** – The voting email has been sent to the Emergency CCB distribution list, and approvals are pending.
- **CCB Hold** – The CCB does not consider or render a decision on the CR; it can be resubmitted at a subsequent CCB meeting. A hold typically occurs because no one attends to present the change.
- **CCB Ready** – The CR has been reviewed and is ready to be presented to the CCB.
- **CM Reviewed** – The Change Management team has verified that all necessary information has been included in the unauthorized CR.

- **Denied** – The CCB or Emergency CCB has denied the CR. It must be returned to Draft status and resubmitted at a later date, or it must be cancelled. Though extremely rare, this decision may result if CCB members have objections to the change that cannot be resolved, either during the meeting or in offline discussions.

- **In CM Review Pending Update** – The Change Management team has determined that the CR is missing information and/or needs clarification.

- **To Be Determined** – The CCB grants conditional approval, with the expectation that the information identified as missing or inadequate during the meeting is provided prior to the planned start of the change. The individuals responsible for these CRs must contact the Change Management team before moving forward so the CR can be reviewed and the CCB decision updated to Approved.

IT Service Management Responsibilities

The ITSM Team is responsible for the maintenance of records to support configuration auditing of the DPS IT System. This includes the dissemination of reports and metrics of the Change Management System database (and in the future, the CMDB) when requested by IT management. Without good information, the business can't look back to know why we did a change. The CMDB will be unreliable if the information is not kept current.

Document Revision

See CM-000 Document Revision

CM-011_ITSM_Terminology_and_Test_Results_Guidelines

Information Technology Service Management

Document Version Date:
11 April 2016

TABLE OF CONTENTS

Purpose

This document contains phrases that may be used in the change request review processing, completing the test results documentation, and outlining the required documentation for test result verification as needed. This list is not intended to be inclusive of all circumstances that may occur, but merely as a good starting point. View them as templates and change as the circumstances require.

References

CM-019 CR Review Process

QA Supported DPS Applications

Typical phases for analyzing CRs

STANDARD CR words: *This CR was analyzed (ITSM CM000) for scope, impact, and change magnitude and deemed a Standard CR. This change will be processed via Standard CM procedures.*

FYI CR words: *This CR was analyzed (ITSM CM000) for scope, impact, and change magnitude and deemed an FYI CR. CCB Blanket approval has been given (ITSM CM000). The individual responsible (whether CM/developer/vendor/systems/DBA/operations…) may start this change when ready. Please comment the CR when the change is completed to notify CM to complete the processing.*

{**Note:** If the FYI does **not** meet the FYI Criteria then the CR should be **re-submitted** in the SDE Change Request System as either a Standard or Emergency CR with the appropriate comment.}

EMERGENCY CR words used after reviewing a submitted Emergency CR: *This CR was analyzed (ITSM CM000) for scope, impact, and change magnitude and deemed an Emergency CR. This change will be processed via emergency CM procedures (ITSM CM000).*

.

EMERGENCY CR words added after receiving the necessary email approval responses: *CCB Emergency approval has been given. The individual responsible (whether CM/developer/vendor/systems/DBA/operations/…) may start this change when ready. Please comment the CR when the change is completed to notify CM to complete the processing.*

The Quality Assurance (QA) Team

*The QA team is responsible for testing certain applications. If the Change Request is in reference to promoting software application changes verify that the changes have been tested by the appropriate QA person. Please see **QA Supported DPS Applications** Excel spreadsheet for the name of the QA person responsible for testing the change. If the application is not listed please contact the QA Lead responsible* *for supporting the area. The QA Leads are located under the QA LEADs tab of the QA Supported DPS Applications document. If you are still unsure, contact the QA manager prior to completing the change request review. Contact the Documentation Librarian if changes are required on the QA Supported DPS Application list.*

Test Results

Test Results – This response is extremely important and may differ greatly depending on the circumstances. (Note: Do not use the word "development" when referring to test results/evidence for <u>any</u> auditable CR) **Below are some possible scenarios and statements that may be used, but only if they are true**. This list is not intended to be inclusive of all circumstances that may occur, but merely as a good starting point. View them as templates and change as the circumstances require.

When the answer is "*Yes*" – indicating that there are already **staging** results attached, there needs to be:

- an attachment that is <u>obvious</u> (e.g., *staging.doc test results)*
- a statement indicating where to find the test results/evidence; examples might include (but not be limited to)::
  - *See attachment abc.txt for test results*
  - *See attachment in MSRxxxxx for test results*
  - *See test results in history from mm/dd/yyyy*
  - *See link to the Central Documentation site*

When the answer is "*No*" or *"NA"* (or even if answered "***Yes***", **but the only test results will be from production and will be added post-deployment)** – indicating that it is impossible to perform **staging** (pre-production deployment) tests we need the following:

- A really good <u>reason/explanation</u>
- Some kind of <u>post deployment</u> <u>results/evidence/explanation</u> **and**
- Some **"<u>good audit words</u>".**

In these cases remember to double-check the CR before closing it to ensure the post-deployment evidence/results **have been attached and that the response to the testing question indicates where to find these test results** (i.e., post-deployment testing results are attached). Some acceptable statements **most applicable to Standard CRs** would include (but not be limited to) the following examples – Please adjust as necessary to "fit" the relevant situation:

- ***AD – Group Policy***

Testing cannot be performed on this Active Directory Group Policy change because this is a "pure production" change. If AD continues to perform as it did before after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***System:***

Testing cannot be performed on this System change because this is a "pure production" change. If the system/server comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

Testing cannot be performed on this network device change because this is a "pure production" change. If the network device comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***System:***

Testing cannot be performed on this System change because this is a "pure production" change that is done through an outside vendor. If the services comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Removal of System****:*

Testing is not expected on powering down systems, networks, and applications. These are being decommissioned and not expected to be used. This was discussed and agreed upon in CCB.

- ***System or database:***

Testing can not be performed on this DB change because this is a "pure production" change. If the database comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***System patch:***

Pre-testing can not be performed on this System change because this is a system patch. If the system/server comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Routine system task (upgrade):***

This is a routine system upgrade task and as such can not be pre-tested. No code changes are involved. This will be installed first on development servers and then if successful will be applied to staging and/or production servers. If the system/server comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Routine system task (applying monthly MS patches):***

This is a routine system task to apply monthly MS patches and as such can not be pre-tested. No code changes are involved. This will be installed first on development servers and then if successful will be applied to staging and/or production servers. If the system/server comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Routine System task of imaging and deploying new servers:***

This is a routine system task to image and deploy new servers and as such can not be pre-tested. This is a routine system task and no code changes are involved. If the servers come up and function as expected, then this is considered an adequate test. This was discussed and agreed upon in CCB.

- ***New Application:***

No pre-testing can be performed on the first time installation of an application on a server. Post deployment test results/evidence will be added by the appropriate personnel upon production release of this CR. This was discussed and agreed upon in CCB.

- ***Application:***

No staging tests can be performed on this upgrade/change, since there is no staging environment for this application. Post deployment test results/evidence will be added by the appropriate personnel upon production release of this CR. This was discussed and agreed upon in CCB.

- ***Application:***

No staging tests can be performed on this change, since we can't reproduce the error in staging. Post deployment test results/evidence will be added by the appropriate personnel upon production release of this CR. This was discussed and agreed upon in CCB.

- ***Application:***

No staging tests can be performed on this upgrade, since there is no staging environment for this application No production applications will be affected by this upgrade until and unless they are reconfigured to call and utilize this upgrade; this will require separate CRs to be submitted and tested before approval would be given. Therefore, implementing this CR will have no impact on any currently running application. This was discussed and agreed upon in CCB.

- ***Performance enhancement:***

Pre-production tests can not be adequately performed on this performance enhancement CR, because in the staging environment for this application there is no way to duplicate the load of a production system. So long as no negative impact is seen in the staging or the production environments, the deployment is considered to be successfully tested. This was discussed and agreed upon in CCB.

- ***Routine maintenance task:***

This is a routine maintenance task; standard/written procedures will be followed. This was discussed and agreed upon in CCB.

- ***Routine third party(vendor)software:***

This is a routine third party (vendor) software task; standard/written procedures will be followed. This was discussed and agreed upon in CCB.

- ***Routine DB task:***

This is a routine DBA (database) task. No code changes are involved and pre-testing has been performed. This change is being made utilizing standard DBA commands that are well documented. There is no way to capture the results of said commands. This was discussed and agreed upon in CCB.

- ***Equipment:***

Testing cannot be performed on equipment request/change because this is a "pure production" request/change. Equipment are routinely added or swapped in this environment. If the equipment comes up after the change is applied, then that qualifies as a successful test. This was noted and agreed upon in CCB.

- ***Monitoring***

This is a routine monitor setup task and as such can not be pre-tested. No code changes are involved. If the system/shows up in monitoring tool after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Networking:***

Testing can not be performed on this Networking request/change because this is a "pure production" request/change. If the network comes up after the change is applied, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Networking (switches):***

Testing can not be performed on this routine Networking request/change for switches because this is a "pure production" request/change. Switches are routinely added or swapped in this environment. A Design Review was held as indicated to ensure configuration was to standard. This was noted and agreed upon in CCB.

- ***Networking (devices):***

Testing cannot be performed on networking devices request/change because this is a "pure production" request/change. Devices are routinely added or swapped in this environment. A Design Review was held as indicated to ensure configuration was to standard. If the network comes up after the change is applied, then that qualifies as a successful test. This was noted and agreed upon in CCB.

- ***Networking (firewalls):***

Testing cannot be performed on this routine Networking request/change for firewalls because this is a "pure production" request/change. Firewall configuration changes are routinely added or removed in this environment. These are reviewed to ensure configuration was to standard. This was noted and agreed upon in CCB.

- ***Test results can not be captured:***

Testing was performed on this change request, but the results/evidence could not be captured. No negative impact is involved. This was discussed and agreed upon in CCB.

- ***Security Scan***

This Security Scan has been run numerous times by security and is being performed again per DPS requirements. Output from the scan is attached by Security when the scan has been completed. This is the standard procedure and has been discussed and agreed upon in CCB

- ***Routine SysAdmin task:***

This is a routine system task to add memory and rescan the disk only and as such can not be pre-tested. This is a routine system task and no code changes are involved. This was discussed and agreed upon in the Austin CCB.

- ***Routine SysAdmin task:***
This is a routine system task to reclaim an obsolete server by removing old instances and applications and re-imaging the server and as such can not be pre-tested. This is a routine system task and no code changes are involved. This was discussed and agreed upon in the Austin CCB.

- ***Configuration change only:***
No code changes are involved, as this is just a configuration change, and no pre-testing can be performed since this is a "pure" production task. This was discussed and agreed upon during CCB.

- ***System task:***
Pre-testing can not be performed on this System change because this is a "pure production" change. If the system/server comes up after the change is applied, then that qualifies as a successful test. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Database task:***
Pre-testing can not be performed on this DB change because this is a "pure production" change. If the DB comes up after the change is applied, then that qualifies as a successful test. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine maintenance task:***
This is a routine maintenance task; standard/written procedures will be followed. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine maintenance task of providing backup:***
This is a routine systems task of ensuring adequate backup; standard/written procedures will be followed. This was discussed and agreed upon in CCB. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine DB task:***
This is a routine DBA (database) task. No code changes are involved and no pre-testing can be performed. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine DB task – creating a new database:***

Pre-testing can not be performed on this CR because this is involves building a NEW database. If the new database creation goes smoothly and can be accessed, then that qualifies as a successful test. This was discussed and agreed upon in CCB.

- ***Routine DB task to temporarily add table space:***
This is a routine DBA (database) task of temporarily adding table space. No code changes are involved and no pre-testing can be performed. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine SysAdmin task (adding users or updating accounts):***
This is a routine SysAdmin task (setting up user accounts and/or granting admin rights to specified users on specified servers only); standard/written procedures will be followed. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine SDE Admin task involving only a configuration change:***
This is a routine SDE Admin task. No code changes are involved, as this is just a configuration change, and no pre-testing can be performed since this is a "pure" production task. “Before” & “After” screenshots will be attached by the SDE Admin after implementation. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System task of adding disk space:***
This is a routine system task to add disk space only and as such can not be pre-tested. This is a routine system task and no code changes are involved. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System task of imaging and deploying new servers:***
This is a routine system task to image and deploy new servers and as such can not be pre-tested. This is a routine system task and no code changes are involved. If the servers come up and function as expected, then this is considered an adequate test. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System task of adding new queues:***
This is a routine system task to add new queues and as such can not be pre-tested. This is a routine system task and no code changes are involved. If the queues function as expected, then this is considered an adequate test. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System task of re-imaging/cloning dev/staging servers:***
This is a routine system task to clone dev/staging servers and as such can not be pre-tested. These servers are not for production, just for development and staging. This is a routine system task and no code changes are involved. If the servers come up and function as expected, then this is considered an

adequate test. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System Root Password change:***
  This is the routine system task of changing the root password, and can not be pre-tested. This happens at least quarterly in compliance with AMD security regulations and no code changes are involved. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine System Admin Password change:***
  This is the routine system task of changing the Admin password, and can not be pre-tested. This happens at least quarterly in compliance with AMD security regulations and no code changes are involved. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine CM task:***
  This is a routine CM task to allow the reconciliation report to run in the necessary environments. This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine CM task:***
  This task is to simply add a new code control repository, and as such can not be pre-tested. This is a routine CM task and no code changes are involved. . This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Routine CM task:***
  This task is to simply add code to an existing SVN repository, and as such can not be pre-tested. This is a routine CM task and no code changes are involved. . This type of FYI CR has been previously discussed and agreed upon as routine and has no impact on the CCB Blanket Approval process.

- ***Telephony Change:***
  Testing cannot be performed on this routine Telephony request/change for phones because this is a "pure production" request/change. Phone additions/changes l are routinely added or removed in this environment. If the phone comes up after they are installed, then this is considered a valid test. These are reviewed to ensure configuration was to standard. This was noted and agreed upon in CCB.

- ***Active Directory:***
  Testing cannot be performed on this Active Directory Group Policy changes because this is a "pure production" change. If AD continues to perform as it did before after the change is applied, then that qualifies as a successful test.

- ***Deactivating Server, network device:***
  Testing is not expected on powering down systems, networks, and applications. These are being decommissioned and not expected to be used. This was discussed and agreed upon in CCB.

Document Revision History

Change 0

Version 1.0.0, January 13. 2011
Initial Document Release; *Author: Paul Urban*

Change 1

Version 1.0.1, June 23, 2011
Update Active Directory Group Policy Object and Firewall changes; *Author: Paul Urban*

Change 2

Version 1.0.2, June 23, 2011
Added equipment updates ; *Author: Paul Urban*

Change 3

Version 1.0.3, September 8, 2011
Added Out-Of-Cycle approval ; *Author: Paul Urban*

Change 4

Version 1.0.4, September 8, 2011
Updated systems and AD words ; *Author: Paul Urban*

Change 5

Version 1.0.5, October 19, 2011
Added Deactivation Words ; Author: Paul Urban

Change 6

Version 1.0.6, October 31, 2011
Removed Emergency from Out-of-Cycle CRs.; Author: Paul Urban

Change 7

Version 1.0.7, December 27, 2011
Renamed ITSM CCC-011; Author: Paul Urban

Change 8

Version 1.0.8, January 25, 2012
Added Telephony quote; Author: Paul Urban

Change 9

Version 1.0.9, August 6, 2012
Correct Security Scan; *Author: Paul Urban*

Change 10

Version 1.0.10, April 6, 2015

Removed references to outdated documentation, “out-of-cycle” standard CR information, and updated format to reflect current standards; *Author: Susie Miller*

Change 11

Version 2.0.0, April 11, 2016

Added QA team information and a link to the supporting doucmentation; *Author: Susie Miller*

CR Review Process

Information Technology Service Management

Document Version Date:
06 April 2017

TABLE OF CONTENTS

Purpose

The purpose of this document is to describe the Change Request (CR) Review and Approval process from the Information Technology Service Management (ITSM) Change Management (CM) team perspective. This document is a useful tool for anyone initiating, approving, or implementing a CR as it will give an insight to both the Change Control Board (CCB) process and data elements required to comply with the Texas Department of Public Safety (TxDPS) Change Management policy and standards. All CRs implemented at TxDPS require CCB approval prior to implementation. The CR Review process is used to help identify areas within the CR which require additional information or clarification. This process helps ensure the CCB members have the correct information when making decisions on the request. It is Change Management's responsibility to review all CRs and follow up with the affected parties of the CR to help them meet these standards. This should happen before CCB to facilitate the CCB review process. CRs not meeting the requirements are subject to rejection/disapproval.

References

General Manual 26.30.0 (sections 3-12)

CM-000_Change_Management_Policies_and_Procedures

CM-011_ITSM_Terminology_and_Test_Results_Guidelines

CM_32_CR Emergency Approval

CM-040_ITSM_Changing_Approved CRs

CM-014 ITSM Change Request Artifacts Checklist

General CCB Information

The Change Control Board is comprised of IT, Division representatives, and ITSM. The CCB meets regularly for a final review of all change requests.

The CCB can make one of four decisions on all types of CRs. These are reflected in the Change Control Board Decision field on the Detail tab of the CR.

- **Approved** – The CCB approves the CR in its current form, authorizing the change to occur.
- **To Be Determined (TBD)** – The CCB grants conditional approval, with the expectation that the CR's information identified as inadequate is provided prior to the planned start of the change. The individuals responsible for these CRs must contact the Change Management team before moving forward so the CR can be reviewed and the CCB decision updated to Approved.
- **CCB Hold** – The CCB does not consider or render a decision on the CR; it can be resubmitted at a subsequent CCB. A hold typically occurs because no one attends to present the change.

- **Denied** – The CCB or Emergency CCB denies the CR. It must be returned to Draft status and resubmitted at a later date, or it must be cancelled. Though extremely rare, this decision may result if members of the CCB have objections to the change that cannot be resolved, either during the meeting or in offline discussions.

To be presented at the CCB meeting, all Standard and Maintenance CRs with scheduled start times between Wednesday (day of CCB) at 9 am through the following Wednesday at 10 am, must be complete and submitted in Ready to Review status no later than **2:30PM the day prior to CCB**. This allows the CM team time to perform an initial review prior to distributing the agenda to CCB members.

Note: The deadline will change as needed due to holidays, closures, rescheduled meetings, etc.

For information on the CR approval process read CM 32 CR Emergency Approval located in the ITSM SharePoint document library.

CR Review Procedure

Change requests (CRs) may be submitted as one of four types: Standard, Maintenance, Emergency, or FYI. All CRs, regardless of type, must be completed per the CM 000 Change Management Policy and Procedures. Also read CM-014 ITSM Change Request Artifacts Checklist for a high level checklist of potentially required change request information.

The primary differences between CR types are impacts and the approval process procedures. As part of the review, the CM team may determine that a change request qualifies as another type and will work with the initiator accordingly to ensure that the CR is processed correctly. The different types are described in the CR Types section of this document. All CM team members should be familiar with the types in order to conduct proper CR reviews.

All CRs should be verified for compliance as soon as they are submitted as “Ready to Review”. The change management system will send an email to IT_Change_Management Mailbox when a new CR is submitted and when its status is changed to “Ready to Review”. Therefore the CM Team member monitoring the Change Management Mailbox is primarily responsible to acknowledge the submission of a CR and process it or assign it to another member of the Change Management Group for processing. All steps for validating a Change Request for compliance are described in this document.

This document will focus on the Standard, Maintenance, and FYI types. For information on Emergency CR approval procedures read CM 32 CR Emergency Approval documentation.

CR Types

Standard

All standard CR changes must be presented to and approved by the Change Control Board (CCB) at the weekly meeting prior to implementation. This meeting is used to communicate to all IT divisions of the changes that are being made and give an opportunity to discuss any changes that may impact your division. The goal should always be to submit a change as a Standard CR and take it to CCB for approval.

Maintenance

Maintenance change requests are for routine maintenance that occurs in a customer approved, regularly scheduled timeframe. Maintenance CRs follow the CR processing rules. However, even though Maintenance CRs are announced during the CCB meeting, unless someone has a specific question about them, they do not require representation and discussion and will be approved.

Before a change can be submitted as a Maintenance CR, it must first be presented as a Standard CR to the CCB. The implementer/team must have already demonstrated that well-documented processes are available and are being followed via previous changes. The individual presenting the change can request that it be considered maintenance. Once approved by the CCB, the change can be submitted as a Maintenance CR in the future. CRs approved to be Maintenance include the following:

- FAST DISPO TLE Servers: Microsoft updates/restart (e.g., 9949) – CCB approved 04/20/2011
- Weekly NEC AFIS server maintenance (e.g., 9950) – CCB approved 04/20/2011
- AFIS CBM basic weekly maintenance (e.g., 9910) – CCB approved 04/20/2011
- AFIS quarterly cold backup and weekly server maintenance (e.g., 9908) – CCB approved 04/20/2011
- Apply [Month Year] Security Updates to SCCM servers (e.g., 9930) – CCB approved May 2011
- Windows Server Critical & Security Updates - Ongoing Maintenance (e.g., 9884) – CCB approved April 2012
- Windows Updates for Blackberry Servers (e.g., 9525) – CCB approved 04/24/2013
- Update Windows 7 x32 and x64 Workstation images with current patches (e.g., 10117) – CCB approved 10/16/2013
- MorphoTrust-Apply MS and sQL patches to IVS Servers (e.g. 2964) – CCB approved 6/10/2015

Note: If habitual issues arise from a Maintenance CR, it may be removed from the approved list and must be submitted as a Standard CR until stability is demonstrated.

Emergency

Reference the following documentation for the Emergency process: CM-000 Change Management Policies and Procedures and CM-032_CR Emergency Approval.

Note: While rare, when situations warrant it, during the course of an emergency call bridge hosted by the OIC, it is determined that a change is needed to resolve a major issue or outage and it must be done immediately, the attendees of the emergency bridge will become the Emergency CCB. The OIC sends out notification via e-mail with the word "(bridge)" in the subject line and contains the OIC bridge phone number in the body of the e-mail to be used to coordinate the emergency. The CM representative will ask if there are any objections to performing the change. If there are no objections, the CM representative will declare that change approved and will need to obtain a roll of all individuals on the call (this can usually be obtained from the OIC)—these names will represent the Emergency CCB for that change. The implementer must still complete an Emergency CR after the call concludes, however once CM reviews it and ensures it is complete, it will not have to be sent out for approval. The CR can be marked Approved and the list of individuals who represented the Emergency CCB should be attached to the CR. This is the only situation in which approval for an Emergency CR from the Emergency CCB distribution list is not required. This will NOT be an unauthorized change.

FYI

FYI change requests are primarily informational. FYI CRs are in place to allow IT and the business to perform changes that will have no, or very minimal, impact to production systems and the agency. The Change Management team reviews and approves FYI CRs. Approval notifications are sent to the Initiator, Assignee, and OIC, with a carbon copy to Change Management and OIC Supervisors.

FYI CRs cannot result in an outage, downtime, or adversely impact the agency. Whether or not a change can be submitted as an FYI ultimately depends on the extent of the change and its possible impact. Examples of changes that may and may not be submitted as FYI CRs are included below.

Allowed

The following list identifies examples of changes that **could** be submitted as FYI CRs, provided there is no or very low risk associated with them.

- Changes with no or minimal impact.
  - Adding disk space to a server with no service interruption.
  - Minor firewall configurations (e.g., CR 9923).
  - Adding/migrating SVN repositories (e.g., 9308).

  - Active Directory changes that do not cause an interruption of service (e.g., 9659).
  - Low- or no-risk configurations (e.g., CR 9890).
  - Equipment moves with no associated downtime (e.g., CR 9719).
  - Microsoft Exchange rules (e.g., CR 9918).
  - Remove domain controller role (e.g., 9735).
  - Create, remove, or update HEAT quick tickets (e.g., 10045).
- Minimal or non-intrusive database changes.
  - Extend table space.
  - Creating indexes (e.g., 9751).
  - Add a value to a table (e.g., 8894).
- Minimal or non-intrusive application changes.
  - Revise JCL to run a report (e.g., 9889).
  - Revise email addresses embedded in JCL (e.g., 9620).
- Equipment decommissions (e.g., CR 9924).
- Post new or updated reports (e.g., Crystal Reports, HEAT).
  Note: These are only allowable if there are no associated database modifications.
- Changes to non-production systems (e.g., updates made to a development environment).

Not Allowed

Certain changes, regardless of impact or possible downtime, cannot be submitted as FYI CRs. These include but are not limited to the following:

- Production database structural or schema revisions (e.g., 9696).
- Requiring Alchemist promotion (e.g., 9874).
- Requiring Turnover promotion (e.g., 9844).
- Application code (e.g., 9920).
- MPLS conversions (e.g., 9708).
- Adding/swapping devices on the network (e.g., routers, servers, switches, phones).
- Server software/OS upgrades (e.g., 9929).
- Software patches (e.g., 9685).
- F5 configurations (e.g., 9916).

- HEAT UI or functionality (e.g., 9902).
- Adding or removing vCPUs on virtual servers (e.g., 9917).
- Agency-wide Microsoft workstation updates (e.g., 9932).
- Agency-wide Sophos updates (e.g., 9561).
- Power-related Facilities work in a data center (e.g., 9729).
- CRs already approved to be Maintenance CRs.

Note: Exceptions may be granted on a case-by-case basis.

Change Request Risk Assessment

Risk assessment is the process of evaluating the potential impact of a proposed change request (CR). It illuminates the risk that the change poses to DPS IT systems and their components. Evaluating the following risk indicators will help determine the impact level of a CR.
Note: CR initiators and their managers are responsible for the initial risk assessment; however, review by the ITSM team may result in a revision to the impact level.

Visibility

Who will or may be affected by the actions required to accomplish the change and/or by the end result of the change? Visibility gauges the potential for a CR to produce results that are so unsatisfactory that they are visible to external and/or internal users, and to executive management. Affected areas include any DPS business area, IT, Law Enforcement, the public, and any external agencies or organizations that rely on systems maintained and/or controlled by DPS.

Business Impact

What is the potential for the CR to interrupt computer production system availability or degrade response time beyond acceptable limits? Business impact gauges the potential for a CR to impair the agency's ability to accomplish day-to-day operations, where such impairment could jeopardize client deliverables and service.
Note: When considering the business impact, keep in mind the stability and reliability of the affected system(s) as well as if those systems have a history of change-related complications.

Communication

What communication, outside submission of the CR itself, is required as part of the change – preparatory, during, coordination with users or other departments (business or IT), approvals, post implementation, etc.? The more communication required and individuals or areas involved, the higher the potential impact to the agency.

Implementation

How complicated is the implementation? What is the expected degree of difficulty? Is there a known or previously successful implementation process? Thoroughly reviewing the implementation plan not only identifies possible holes in the steps but also allows one to gauge the difficulty, required time, and complexity of the change's coordination. An increase in any of these areas could result in a higher risk to the agency.
Note: Complexity and difficulty are not necessarily the same thing.

Validation

How complicated is the validation plan? Are a lot of individuals necessary in order to perform the validation? In addition to assisting the initiator with determining the scope of the change, the validation plan can also indicate the extent of time that a system may be down due to the length and/or complexity of the tasks required to validate that the change was successful.

Rollback

How complicated and difficult is the rollback plan? This gauges those characteristics of a proposed change that, in the event of a production system failure, reflect the degree of complexity of the rollback plan, the amount of time required for recovery, and the potential for success or failure of the rollback plan. Lack of a successfully proven rollback plan could also pose a higher risk to the agency.

Impact to Mission Critical Operations

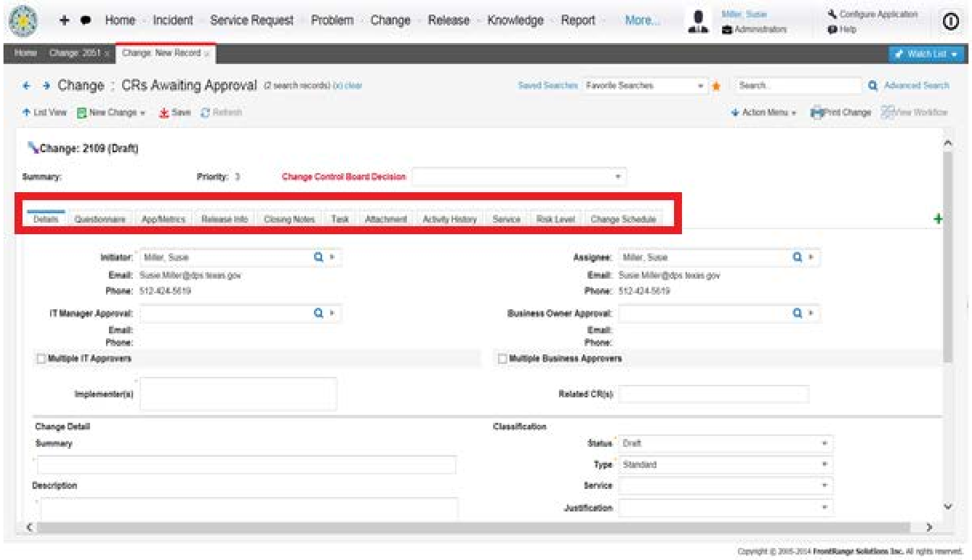
This risk indicator gauges the potential for a change to disrupt any aspect of DPS's production environment and routine operation schedules and procedures.

Change Review Process:

The Change Management System currently in use (HEAT) consists of 11 tabs of which 7 are currently used. Depending on your Role in HEAT, you may or may not have access to all of the tabs. In addition, certain tabs may be hidden. In order to see all available tabs, click on the green plus (**+**) sign located on the right side of the form on the same level as the tabs. You may need to scroll to the right or maximize the window to see it. Information is gathered within each tab outlining the details, areas impacted, implementation, rollback, validation plans and release information. Each tab has required fields on the form which are indicated by an asterisk (*). Tabs with the "(0)" indicates the number of files that are stored within the tab. For example: Attachment (2) lets you know that 2 file attachments exist. Each tab will be discussed in detail the following section.

HEAT Change Request Form Tabs

- Details
- Questionnaire
- App/Metrics
- Affected Groups (Not Reviewed by CM)
- Release Info
- Closing Notes
- Task (0) (Not Reviewed by CM)
- Attachment (0)
- Activity History (0)
- Service (0) (Not Reviewed by CM)
- Risk Level (Not Used)
- Change Schedule (Not Used)



Change : CRs Awaiting Approval (2 search records) (x) clear

Change: 2109 (Draft)

Summary:

Priority: 3

Change Control Board Decision

Initiator: Miller, Susie

Email: Susie.Miller@dps.texas.gov

Phone: 512-424-5619

Assignee: Miller, Susie

Email: Susie.Miller@dps.texas.gov

Phone: 512-424-5619

IT Manager Approval:

Email:

Phone:

Business Owner Approval:

Email:

Phone:

□ Multiple IT Approvers

□ Multiple Business Approvers

Implementer(s)

Related CR(s):

Change Detail

Summary

Description

Classification

Status Draft

Type Standard

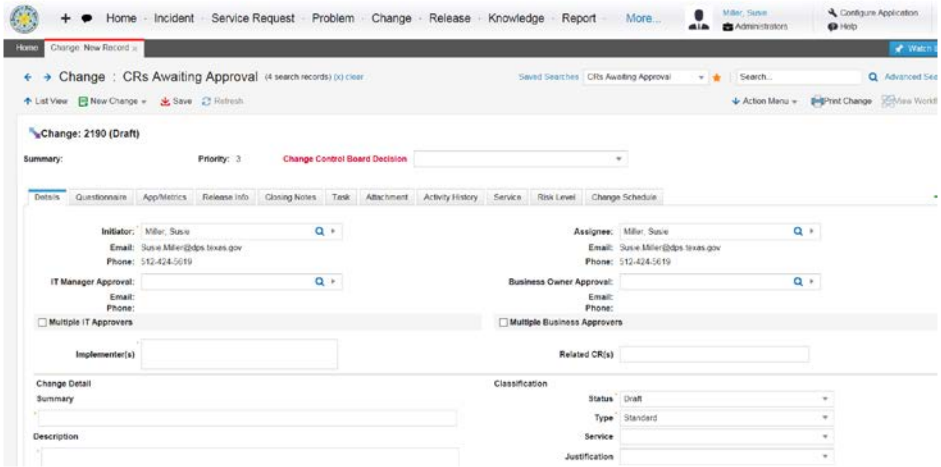
Service

Justification

Copyright © 2005-2014 FrontRange Solutions Inc. All rights reserved.

Details Tab

The upper section contains general information about the CR and the CCB approval status. The lower section is for the CR details.



Change : CRs Awaiting Approval (4 search records) (x) clear

Saved Searches: CRs Awaiting Approval

Change: 2190 (Draft)

Summary:

Priority: 3

Change Control Board Decision:

Initiator: Miller, Susie
Email: Susie.Miller@dps.texas.gov
Phone: 512-424-5619

Assignee: Miller, Susie
Email: Susie.Miller@dps.texas.gov
Phone: 512-424-5619

IT Manager Approval:
Email:
Phone:

Business Owner Approval:
Email:
Phone:

□ Multiple IT Approvers

□ Multiple Business Approvers

Implementer(s):

Related CR(s):

Change Detail

Summary

Description

Classification

Status: Draft

Type: Standard

Service:

Justification:

Initiator (*Required):

Initiator is the requester of the Change. The initiator could be a business area representative. Assignee should take responsibility for a completed CR.

Implementer(s) (*Required):

This is the person/group responsible for implementing the Change. Each name should be separated by a comma ",".

IT Manager Approval(s) (*Required):

IT Manager Approval is a required field. The IT managers of the affected areas, and the managers of the implementers (if other than the affected areas) must approve the CR. Approvals for each manager must be attached to the CR.

NOTE: The IT and Business Approver cannot be the same person. In the event there is no Business Owner, the IT Team Lead or higher can be the Business Approver. In this case, the IT Approver must be that individual's supervisor or above.

Multiple IT Approvers (*Optionally Required):

If the CR change requires more than one implementer the box should be checked and the additional IT Manager(s) should be listed. This field becomes required as soon as the box is checked. Approval emails must be attached for every additional approver listed on the CR.
Note: All Change Requests require both an IT and Business Approver.

Assignee:

The assignee is the person responsible for ensuring the changes are implemented as described in the CR.

Business Owner Approval (*Required):

To ensure visibility and ensure communication and coordination has taken place regarding the CR we require a Business Owner approval. The Business Owner of the affected areas and the managers of the implementers (if other than the affected areas) must approve the CR. Approval must be attached the the change request.

Multiple Business Approvers **(*Optionally Required):**

In the case of having multiple business areas affected, make sure the box is checked and the additional Business Manager(s) are be listed. FYI - This field becomes required as soon as the box is checked. Approvals for every additional approver must be attached to the change request.

Note: All Change Requests require both an IT and Business Approver. The IT and Business Approver cannot be the same person. In the event there is no Business Owner, the IT Team Lead or higher can be the Business Approver. In this case, the IT Approver must be that individual's supervisor or above.

Related CR(s):

Check this field for any related CR(s). Review the CR for any pertinent information related to the current CR.

Change Control Board Decision:

The Change Control Board Decision (CCBD) Field represents the current CCB approval decision and which can only be changed by CM team members. The CM team members can update this field to the appropriate decision during the CR review process. A status of "Ready for Review" will trigger an update to change the Change Control Board Decision to "Awaiting Approval".

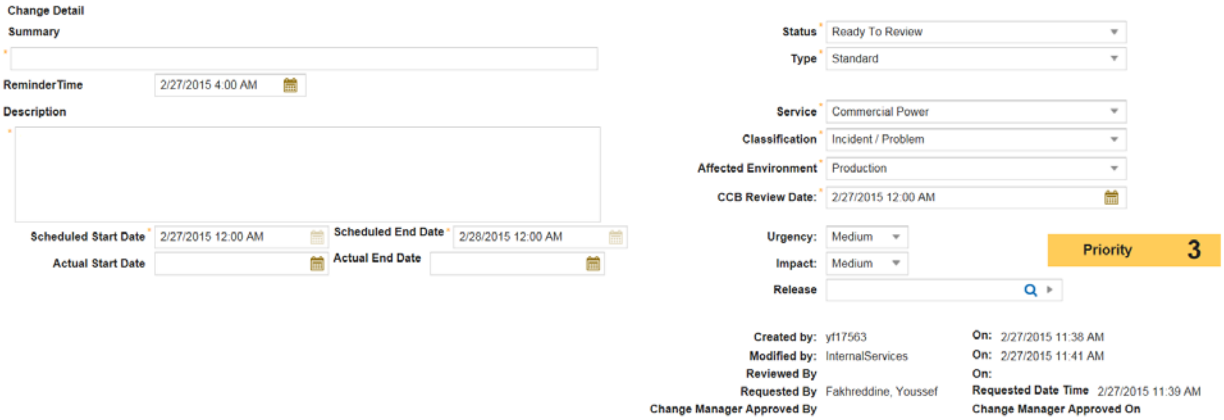
The CM team reviewing the CR can make one of five decisions prior to CCB review.

- **Awaiting Approval** (Used for Standard and Maintenance CR types) –The CR has been submitted and is ready for CM review.
  Note: If a CR is returned to Draft status, the decision is removed.

- **CM Reviewed** (**unauthorized CRs only**) – The Change Management team has verified that all necessary information has been included in the unauthorized CR. This decision is used if an unauthorized change in production has occurred.

- **In CM Review Pending Update** (Used for Standard and Maintenance CR types) – The Change Management team has determined that the CR is missing information and/or needs clarification.
- **CCB Ready** (Used for Standard and Maintenance CR types) – The CR has been reviewed and is ready to be presented to the CCB.
- **Awaiting Emergency Approval** (Used for Emergency CR types) – The voting email has been sent to the Emergency CCB distribution list, and approvals are pending. See CM-032 CR Emergency Approval.

Change Detail



Change Detail

Summary *

ReminderTime 2/27/2015 4:00 AM

Description *

Scheduled Start Date * 2/27/2015 12:00 AM

Scheduled End Date * 2/28/2015 12:00 AM

Actual Start Date

Actual End Date

Status * Ready To Review

Type * Standard

Service * Commercial Power

Classification * Incident / Problem

Affected Environment * Production

CCB Review Date: * 2/27/2015 12:00 AM

Urgency: Medium

Impact: Medium

Priority 3

Release

Created by: yf17563 On: 2/27/2015 11:38 AM

Modified by: InternalServices On: 2/27/2015 11:41 AM

Reviewed By On:

Requested By Fakhreddine, Youssef Requested Date Time 2/27/2015 11:39 AM

Change Manager Approved By Change Manager Approved On

Summary (*Required):

Make sure that the CR has a brief and meaningful Change Summary which reflects the main aspects of the change. It is helpful to include the System/Area/Application which is going to change as well as the reasons for the change. A change title should provide good information what was done if you look at it at any later time.

Description (*Required):

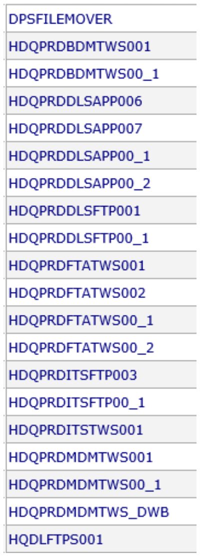
The CR description should describe, in detail, reason/purpose for the CR. The supporting documentation should be placed in the Questionnaire, App/Metrics, and Release Info tabs within the CR.

Read the description very carefully. This information can help you identify potential missing data fields within other tabs of the CR.

Scheduled Start Date and End Date (*Required): Make sure the scheduled times are correct and fall in the CCB review timeframe. If a change spans over several days, a day to day activity plan has to be attached. Include the schedule (CRs spanning multiple days).

NOTE: When reviewing the scheduled start time, any CR that has a start time of 7:00 (am/pm) needs to be rescheduled for 15 minutes before or after. This will allow for OIC shift changes.

Any change request that has TWS agent impact cannot start at 2:00 pm. This includes the following:



DPSFILEMOVER
HDQPRDBDMTWS001
HDQPRDBDMTWS00_1
HDQPRDDLSAPP006
HDQPRDDLSAPP007
HDQPRDDLSAPP00_1
HDQPRDDLSAPP00_2
HDQPRDDLSFTP001
HDQPRDDLSFTP00_1
HDQPRDFTATWS001
HDQPRDFTATWS002
HDQPRDFTATWS00_1
HDQPRDFTATWS00_2
HDQPRDITSFTP003
HDQPRDITSFTP00_1
HDQPRDITSTWS001
HDQPRDMDMTWS001
HDQPRDMDMTWS00_1
HDQPRDMDMTWS_DWB
HQDLFTPS001

Actual Start Date and End Date: The actual start and end dates should be blank. If these dates are filled contact the initiator to find out why.

Status:

All new CRs have the default status "DRAFT". Change Management does not process any DRAFT changes.

FYI and Maintenance CRs -- Status should be set to ***Ready for Review*** .

Standard CR -- Change the status to ***Planned.*** All planned standard CRs will be reported on in the DPS – Planned Change Report and sent every Friday at 2:00pm. Recipients of the report will review the items on the agenda and schedule meetings as needed. The due date for a completed CR is Tuesday by 2:30PM. If a concern is raised the status should be changed back to ***Draft***. If the planned change is moving forward the status should be changed to ***Ready for Review***.

Change Management will review the CR prior to adding it to the Change Control Board (CCB) agenda to ensure it is complete and ***Ready for Review*** by the CCB members.

When a CR is ready for to be reviewed by the Change Management Group, the requester needs to put the change into status ***Ready for Review***.

Available status:

- **Draft** – new CR pending completion
- **Planned** – new CRs that are planned for implementation pending QA/Technical review
- **Cancelled** – a CR which is no longer needed
- **In Progress** – The changes are being implemented
- **On Hold** – The CR has been placed on hold by the initiator, assignee, and/or implementer. This is usually due to unexpected issues encountered prior to actual implementation. It can be used prior to or after CCB approval provided no work has begun. However, CRs on which work has already been performed cannot be placed on hold. If the causes for the hold result in rescheduling, the Change Management team must be contacted first.
  Changes that span multiply days (aka rolling CRs), need to be placed on hold. The CR implementer, assignee or requestor is responsible for contacting the OIC to pause the change. The process will set the CR status to hold.
- **Ready for Review** – Ready for ITSM team member review

The ITSM Team members review only the CRs with a current status of "Ready for Review". A special saved search called "CRs Awaiting Approval" is available for quick access to the list of CRs ready to be reviewed.

Type (*Required):

Change requests (CRs) may be submitted as one of four types: Standard, Maintenance, FYI or Emergency. All CRs, regardless of type, must be thorough, complete, and follow the Change Management process.

ITSM Reviewer is responsible for verifying that the type selected meets the correct categorization of the change.

- Standard
- Maintenance
- Emergency
- FYI

Service (* Required): Verify that the Service meets the correct categorization of the change.

Classification (* Required): Null, (None), Enhancement, Incident/Problem, Release, Scheduled Maintenance, Unscheduled Maintenance. The selected classification should relate to the change being made. If the change is regular monthly maintenance then "maintenance" would be the appropriate selection.

Affected Environment (* Required): Ensure right environment is selected. This should be as specific as possible. E.g. not all changes will affect whole DPS. Choices are: Production, Test, Development, Pilot, QA.

CCB Review Date (* Required): The date the CR will be presented to the CCB.

Urgency and Impact = Priority:

A change request's Priority is calculated using Urgency (High, Medium, Low) and Impact (High, Medium, Low) responses. These should be selected based on the degree of risk associated with the CR. Use the following matrix as an aid to determine the most appropriate impact. For example, a minor HTML update to DPSNET that requires an outage would be high impact. However, if the same update did not require an outage, it would be medium impact.

Use the following matrix as an aid to determine/verify the most appropriate Urgency and Impact are selected. Make sure to review this. Be alert if Low is selected. Note: ITSM reviewer may make revisions to these fields. The Priority is calculated from a combination of these fields.

Level	**Visibility**	**Business Impact**	**Communication**	**Implementation**	**Validation**	**Rollback**	**Training Required**	**Impact to Mission Critical Applications**
High	Agency-wide; external DPS customers	Agency-wide	Agency-wide; multiple departments/ business areas	Multiple business areas, systems affected; multiple teams required for release	Difficult/complex/ lengthy	Difficult/complex /lengthy	Extensive	Major
Medium	Multiple business and/or IT areas	Tier 1 applications and/or supporting systems	Multiple areas	Two or fewer business areas, systems affected; two or fewer teams required for release	Moderate difficulty/ complexity/length	Moderate difficulty/ complexity/length	Minimal	Moderate
Low	Single business and/or IT area	Non-tier 1 applications and/or supporting systems	One area or none required	One business area, system affected; one team required for release	Basic/easy/short	Basic/easy/short	None	Minor

High Impact Criteria

High impact changes pose a significant level of risk for potentially affecting multiple user groups and/or systems. They are usually highly visible, higher priorities to the agency, and/or require greater attention when they are rolled out to production. Changes that are considered high impact include those with any of the following characteristics:

- Affect multiple existing tier 1 systems, including implementing new systems (e.g., CR 10053: Sophos Updates).
- Scheduled to occur during standard business hours (Monday-Friday, 8 am-6 pm Central) or during critical processing periods as determined by the business (e.g., CR 10271: Satellite System Outage).
- Could affect more than one department, IT area, set of customers, or possibly all users (e.g., CR 10119: Upgrade au_ims_s004_tmp.tle.dps (DPSNET) to Windows 2003R2).

- Highly visible to external and/or internal users and executive management (e.g., CR 9785: Annual update of F5 Certificates).

- Include complicated and/or lengthy installation times (e.g., CR 9747: Migrate Exchange databases).

- Include complex and lengthy, difficult, or impossible rollback plans (e.g., CR 9904: Quarterly Mainframe Initial Program Load (IPL)).

- Require training to use the function or system that is being implemented (e.g., CR 10366: FPS Pilot Implementation)

Medium Impact Criteria

Medium impact changes pose a moderate or standard, but manageable risk for potentially affecting multiple user groups and/or systems. Changes that are considered medium impact would include

- Revisions to existing functions of a hardware or software component (e.g., CR 10115: LRS Contact Center Phone Routing Update).

- Most modifications to a system that do not affect critical Tier 1 applications or associated hardware (e.g., CR 10131: Apply Existing Group Policy to DPS Computers)

- Modifications to a production batch system that does not have critical production deadlines (e.g., CR 10174: Modify Batch Request JCL)

- Maintenance to minor systems software (patches) (e.g., CR 10254: Windows Updates for Blackberry Servers).

- Those that are visible to multiple customers (e.g., CR 10231: SDE - Add error checking to the IT3 process).

- Those that might disrupt service to a specific set of customers (e.g., CR 10209: Los Tomates OASIS to Mobile Cad EM conversion).

- Those where rollback is somewhat difficult and lengthy but with a high probability of success (e.g., CR 10243: Deploy DLS 2.13.11b5).

- Those that are controlled by a third-party vendor (e.g., CR 10242: TLETS Spill Queue-CPI).

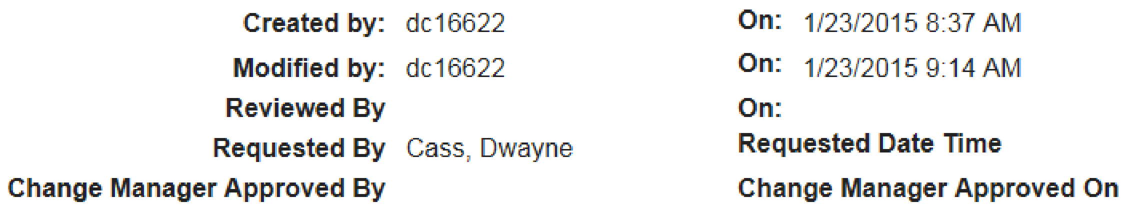
Low Impact Criteria

Low impact changes pose a minimal risk for potentially affecting multiple user groups and/or systems. These include changes with limited visibility or impact on day-to-day system operations and maintenance. Examples of low impact CRs include the following:

- 9960: DBPHRRDT job update
- 10132: HQIMSS050-Stop DNS Server Service
- 10198: Change output from TCIC and CCH monthly and weekly metrics reports to PDF
- 10244: Move 1 DPSDirect Report to Production
- 10260: Decommission Tipping Point "4" R23R1 DC-A
- 10304: Throttle Replication Between Virtual Tape Library (TL1) and Virtual Tape Library (VTL2 V2)
- 10309: Decommission HQIMSS050
- 10320: DLS access for new Lubbock Regional office

Release: This field is not currently used.

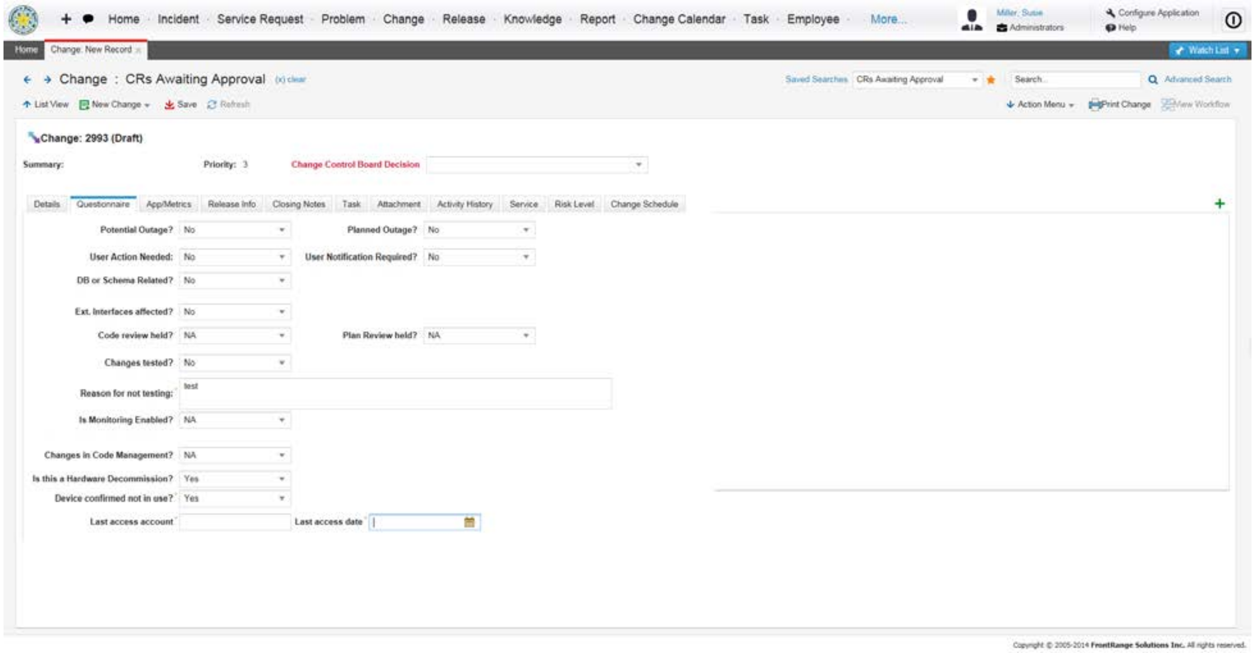
At the bottom of the form you can see the ACID for the initiator and date the CR was created, who modified it last and date and time, the ITSM CM team member who reviewed the CR for completeness and the date and time this was saved, the name of the initiator, the Requested Date and Time could be the time the CR was status was set to “Ready for Review”, the Change Manager Approved by is the person who set the CR to CCB ready and lastly, the Change Manager Approved On is the CCB member who approved the CR.



Created by:	dc16622	**On:**	1/23/2015 8:37 AM
Modified by:	dc16622	**On:**	1/23/2015 9:14 AM
Reviewed By		**On:**	
Requested By	Cass, Dwayne	**Requested Date Time**	
Change Manager Approved By		**Change Manager Approved On**	

It is the responsibility of the ITSM CM team member to verify that the CR meets the correct impact criteria as specified in document **CM-000_Change_Management_Policies_and_Procedures**

Questionnaire Tab



Change: 2993 (Draft)

Summary:		Priority:	3
Change Control Board Decision			
Potential Outage?	No	Planned Outage?	No
User Action Needed:	No	User Notification Required?	No
DB or Schema Related?	No		
Ext. Interfaces affected?	No		
Code review held?	NA	Plan Review held?	NA
Changes tested?	No		
Reason for not testing:	test		
Is Monitoring Enabled?	NA		
Changes in Code Management?	NA		
Is this a Hardware Decommission?	Yes		
Device confirmed not in use?	Yes		
Last access account		Last access date	

The Questionnaire Tab is used to document any potential/planned outages, identify users affected and actions they may need to take, list external interfaces that may be impacted by the change, document the code and/or peer review, document the testing of the change, the monitoring tool used and list where the code is stored. All questions are mandatory, meaning they must be addressed.

Sometimes NA is an acceptable answer, but usually **Yes/No** is more applicable. For Example, No downtime is more definitive than NA downtime.

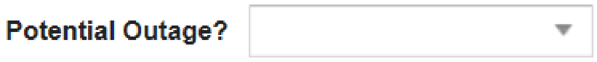
The following table may serve as a guide as to which questions can be NA for various work areas.

Questions from Questionnaire Tab

Work Areas	DB or Schema Related	Code/Peer Review
System/Server CR	NA	NA
Network CR	NA	NA

Potential Outages

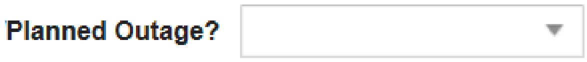
Is there a risk of an unplanned outage or downtime? If so, state the type of potential impact, and estimate of outage, and known systems/services/areas that can potentially be impacted.



Potential Outage?

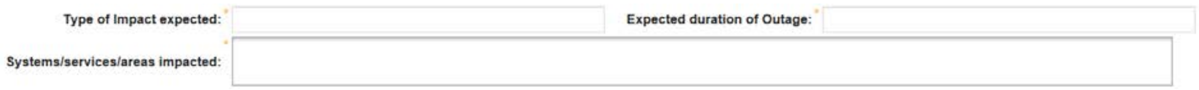
Planned Outages

Does the change require downtime? If so, state the type of impact expected, expected duration of outage, and systems/services/areas impacted.



Planned Outage?

If either potential or planned outage are selected as "**Yes**", the following information will need to be provided.



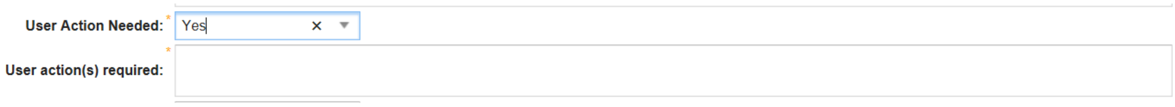
Type of Impact expected: *

Expected duration of Outage: *

Systems/services/areas impacted: *

User Action Needed:

Does the change require a user to take an action? If "**Yes"**, check the "**User action(s) required:"** text field for detailed instructions the user must take to address the need. In addition, **User Notification Required** should be "**Yes**" and user notification email containing the instructions must be attached.

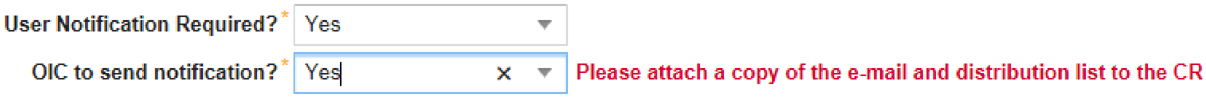


User Action Needed: * Yes

User action(s) required: *

User Notification Required?

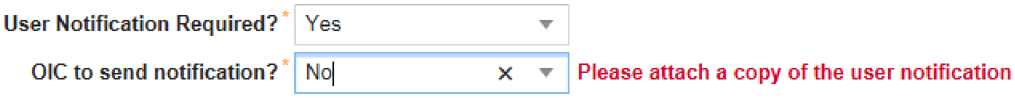
If users are required to take an action or if users are going to experience downtime due to the change, Users should be notified via e-mail. If "**Yes"**, a second question will appear asking if the OIC will be responsible for sending the user notification. If "**Yes**", a message will appear telling the user to attach a copy of the e-mail and distribution list to the change request. If "**No**", a message will appear telling the user to attach a copy of the user notification. The email can be attached after CCB has approved the CR but before implementation of the CR.



User Notification Required?* Yes

OIC to send notification?* Yes

Please attach a copy of the e-mail and distribution list to the CR



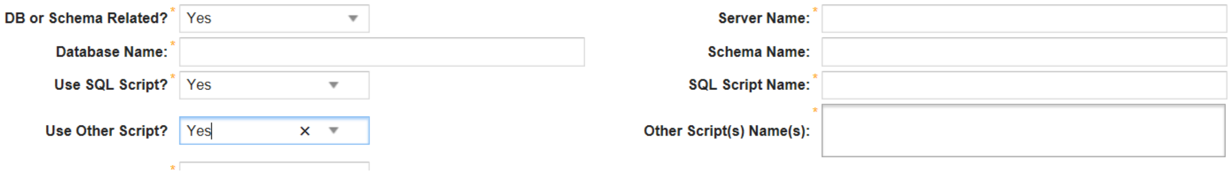
User Notification Required?* Yes

OIC to send notification?* No

Please attach a copy of the user notification

DB or Schema Related?

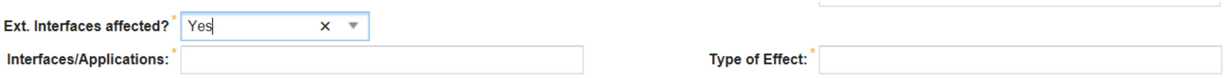
If the CR requires DB or Schema changes the details surrounding the change should be documented within under the DB or Schema Related question. This section has additional requirements which depend on the answer to the question. Each field should be verified.



DB or Schema Related?*	Yes	Server Name:*	
Database Name:*		Schema Name:*	
Use SQL Script?*	Yes	SQL Script Name:*	
Use Other Script?	Yes	Other Script(s) Name(s):*	

Ext. Interfaces affected?

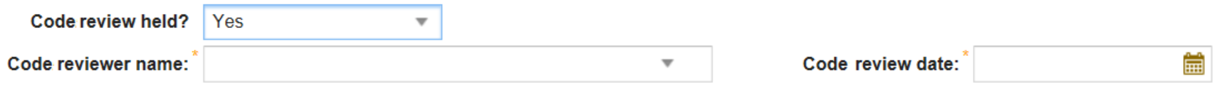
Are external interfaces or applications affected? Does this application touch another application? Will taking out this service affect another service? If the answer is "**Yes"**, the other affected interfaces/applications and type of effect should be listed.



Ext. Interfaces affected?*	Yes		
Interfaces/Applications:*		Type of Effect:*	

Code review held?

Ensure that changes have undergone a code review. Appropriate responses are Yes, No, and NA. A Yes response will enable the Code reviewer name field. Complete this field with the name of the person who reviewed the change. This normally should not be the same person as the implementer.



Code review held? Yes

Code reviewer name: *

Code review date: *

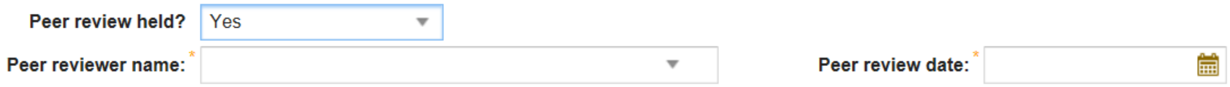
If the response is “**No”**, the reason should be stated in the “Reason for no review” box.

If the response is “**NA**” or “**No**”, a peer review should be completed.

Peer review held?

Ensure that the CR has undergone a peer review. The peer review consists of a review of the implementation plan, verification plan, schedule, and rollback plan. The peer reviewer should be an individual knowledgeable in the area that the change relates to. If a code review is not performed a peer review will be required.

Appropriate responses are Yes, No, and NA. A Yes response will enable the Peer reviewer name field. Complete this field with the name of the person who reviewed the change. This normally should not be the same person as the implementer.



Peer review held? Yes

Peer reviewer name: *

Peer review date: *

If the response is “**No”**, the reason should be stated in the “Reason for no review” box. If “**Yes”**, the name of the person conducting the review and date should be entered.

Code and Peer Review Descriptions

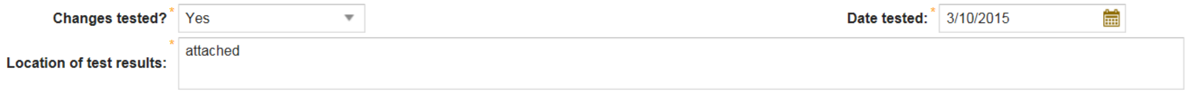
- Code Review
  - Ensure that any code and scripts have been reviewed and approved by another individual knowledgeable in the area that the change relates to;
  - Ensure that all code and scripts have been stored in an approved version control management system (i.e. SVN) and provide link to the specific tag in the repository, or, if stored in the trunk, indicate the revision number;
  - If an SVN repository is unavailable, store items in a network location accessible to Change Management staff. If there is no other location available, items may be attached to the Change Request, however they should be stored in a format that will not allow accidental execution, i.e. SQL scripts should be stored as.txt.

- Peer Review
    - Ensure that all plans (implementation, rollback, and validation) and schedules related to the change have been reviewed and approved by another individual knowledgeable in the area that the change relates to.

Change tested?

Was the change tested? If **"Yes"**, the test results should be attached to the change request. The "location of test results" should simply state that the test results are attached.

Links to test results will only be allowed when the location is not subject to change. In this case, a link to the test results should be listed in the "location of test results" box.

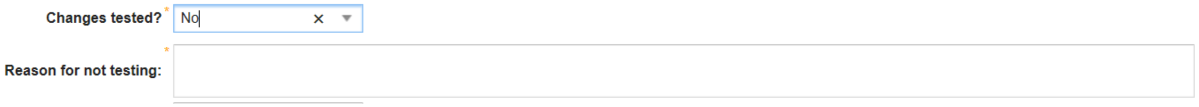


Changes tested?* Yes
Date tested:* 3/10/2015
Location of test results:* attached

If the answer is **"No"** a reason should be entered in the "reason for not testing" box. Please note that some changes cannot be tested. This is appropriate in some cases. Please refer to the correct wording documentation for the acceptable verbiage and additional information on required documentation.

CM-011_ITSM_Terminology_and_Test_Results_Guidelines

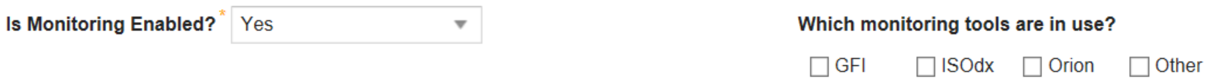
Note: All changes are expected to have test results attached to the CR. Links to test results will only be allowed when the location is not subject to change. For example, links to SharePoint are acceptable when the document is stored in a location where it will not be updated, changed, or deleted. Where QA is part of the process, QA must sign off in order for changes to receive Approval.



Changes tested?* No
Reason for not testing:*

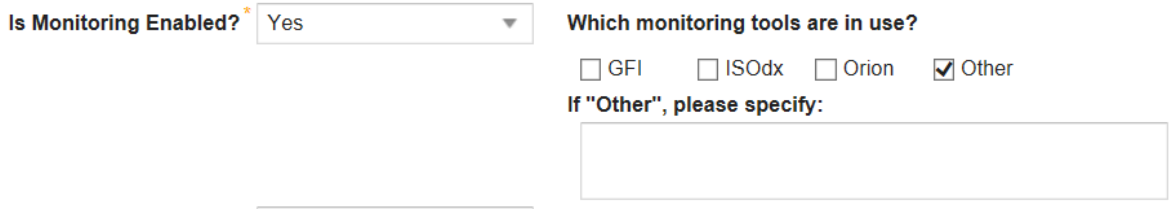
Is Monitoring Enabled?

Critical systems and environments should be monitored when being impacted by a change. Verify that the question has been answered. Appropriate responses are **Yes, No and NA**. Remember, all critical systems in our environment should be monitored. When **"Yes"** is selected a conditional question is asked. Make sure a monitoring tool is selected when the response is "**Yes**". Although "**NA**" is an option, more information should be obtained from the requester as to why the system is not monitored. The answer should be changed to "**No**" and the reason for no monitoring should be added to the "Reason for not monitoring" field that appears.



Is Monitoring Enabled?* Yes
Which monitoring tools are in use?
□ GFI □ ISOdx □ Orion □ Other

If "**Other**" is checked, an additional "If other, please specify" box will appear. The monitoring system should be identified in that box.



Is Monitoring Enabled?* Yes

Which monitoring tools are in use?

□ GFI □ ISOdx □ Orion ☑ Other

If "Other", please specify:

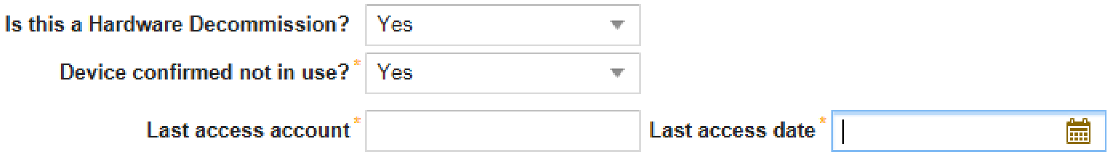
Is this a hardware decommission? This is a simple **yes** or **no** question. Make sure you have read and understand the CR description very carefully as it may indicate hardware decommission is required. If it states a hardware decommission is required the selection should be “**Yes”**.

NOTE:

- The server owner is responsible for verifying the system is no longer in use prior to submitting a service request to decommission the server.
- Insure that the Server Team has conducted a validation that the server is not being logged on to, accessed by a process account, or communicating with a production system that would be taken down when the decommission happens.
- If the Server Team determines there is a possible conflict, they are to contact the appropriate area. If there is no conflict detected, the Server Team will submit the Change Request for to decommission the server**.**

When the response is “**Yes**”, additional required fields will appear.

Device confirmed not in use – Yes or No response is to ensure the device was monitored and verified is no longer in use.
Last access account – ACID or account that last accessed the device.
Last access date – The date the device was last accessed.

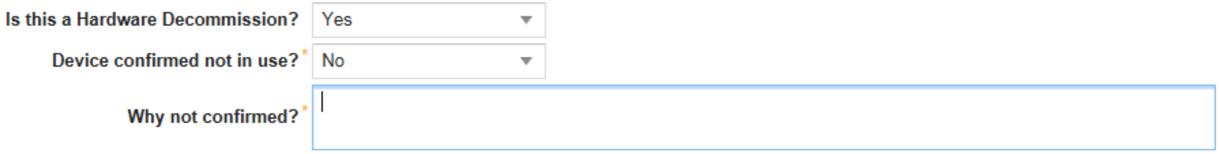


Is this a Hardware Decommission? Yes

Device confirmed not in use?* Yes

Last access account* Last access date*

If the response to the “Device confirmed not in use?” is “**No**”, a reason for not confirming the non-use is required.



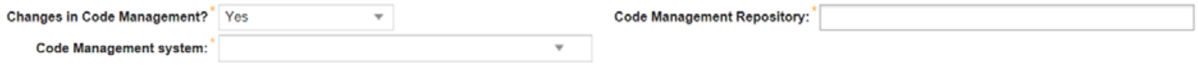
Is this a Hardware Decommission? Yes

Device confirmed not in use?* No

Why not confirmed?*

Changes in Code Management?

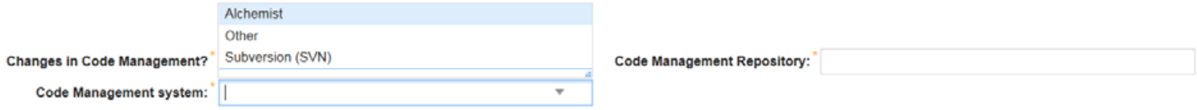
This question is in reference to the version control of code. Appropriate responses are **Yes, No** and **NA**. All code changes should be stored in an approved version control system. The system should be selected from the Code Management System drop down box. If no repository is available for the project, the developer should contact the version control system administrator for assistance setting up their project. Typically, Alchemist is the approved code management system for mainframe changes and SVN is the approved code management system for all other artifacts. In rare cases, the submitter may choose "other" and an alternative version control system may be named. A link to the code should be listed in the Code Management Repository box. The CR may not be approved for CCB if the appropriate version control system is not provided. You need to verify that the code is accessible and URL is valid. Remember that if the link provided points to the "trunk", a revision number must be provided. If the link points to a "tag", no revision number is needed.



Changes in Code Management?* Yes

Code Management system:*

Code Management Repository:*

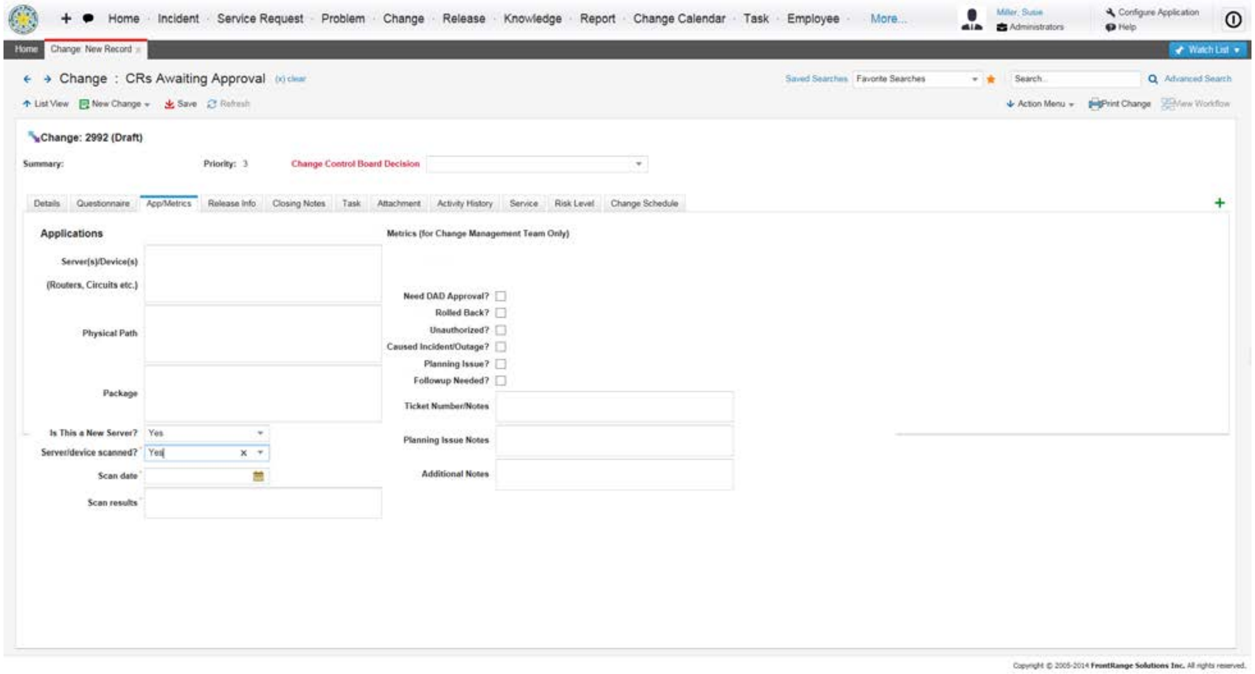


Changes in Code Management?*

Code Management system:*

Code Management Repository:*

App/Metrics Tab



Change: 2992 (Draft)

Summary:

Priority: 3

Change Control Board Decision

Applications

Server(s)/Device(s)
(Routers, Circuits etc.)

Physical Path

Package

Is This a New Server? Yes

Server/device scanned? Yes

Scan date

Scan results

Metrics (for Change Management Team Only)

Need DAD Approval? □
Rolled Back? □
Unauthorized? □
Caused Incident/Outage? □
Planning Issue? □
Followup Needed? □

Ticket Number/Notes

Planning Issue Notes

Additional Notes

The App/Metrics tab is used to document which servers, devices or applications are impacted by the change as well as the file location and package names that are used for the change. Below is a list of possible entries for the Server, Physical Path and Package text boxes.

Servers/Devices
(Routers, Circuits etc.): Name(s)/IP(s) of physical or virtual servers or other devices affected by the change. If the list is lengthy, an attachment may be added to the CR listing the names and a note put in the Servers field indicating there is an attachment.
Physical Path: Path(s) to the specific locations on the server(s) and/or device(s) that are being affected.

Package: A list of the packages to be deployed during the change should be listed.

Is This a New Server?: All web applications and all devices added to the network with the exception of PC's and laptops require a vulnerability scan:

1. Servers to include virtual servers
2. Firewalls
3. Switches
4. Routers
5. Intrusion Detection System
6. Intrusion Prevention Systems
7. Databases
8. Any device requiring an IP address

If it is not a new server or device the selection should be "**No**". If the server or device is new to the network, the response should be "**Yes**". Three sub-questions will appear which are required:

Server/device scanned?: This question is to validate the new server/device has been scanned.

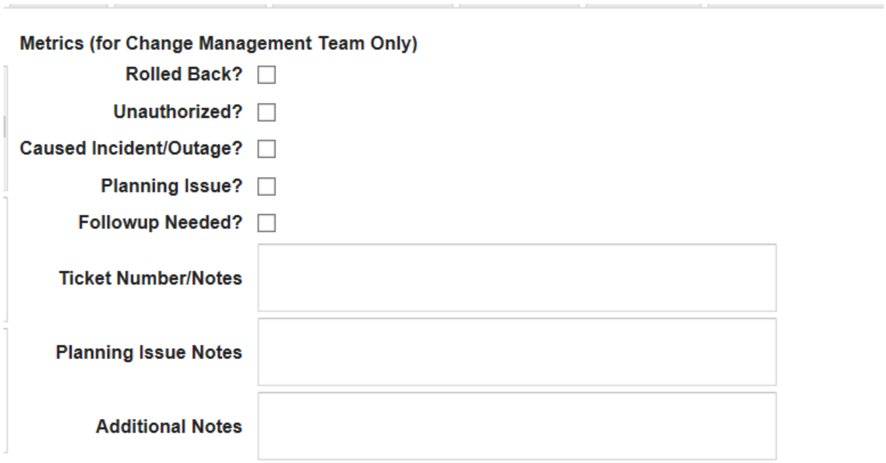
Scan date: The date of the scan.

Scan Results: Results which can be attached to the CR.

Metrics Section

This form includes a Metrics section which is only available to the ITSM CM team. We document events that resulted in a problem during implementation. In addition, it is used to document when follow-up is needed. If the CR indicates a screenshot will be used for validation we check the "Followup Needed" box and enter a description in the Additional Notes text field.

Completing the metrics information enables development of Key Performance Indicator (KPI) dashboards and reports. In addition to the reporting and dashboard capabilities, the form is used for tracking CRs that require follow up.



Metrics (for Change Management Team Only)

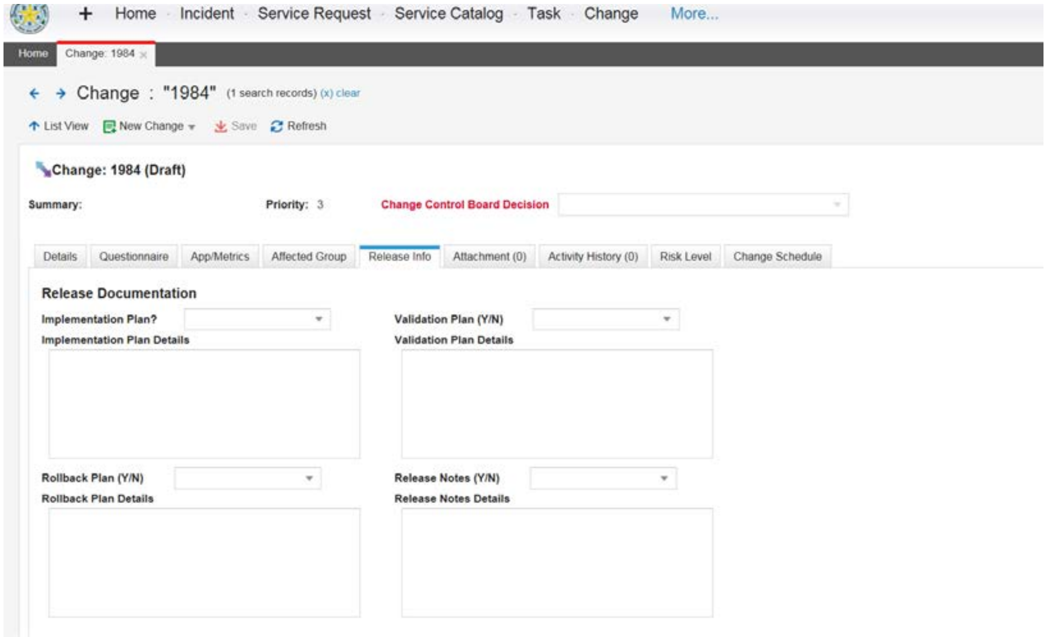
Rolled Back?	□
Unauthorized?	□
Caused Incident/Outage?	□
Planning Issue?	□
Followup Needed?	□
Ticket Number/Notes	
Planning Issue Notes	
Additional Notes	

- **Rolled Back?** – This field is automatically set by the system in the event the status of the CR is set to Rollback-Open or Rollback.
- **Unauthorized?** – An unauthorized change is a change made to a DPS system for which a change request (CR) should have been submitted and approved prior to implementation but was not. Following an unauthorized change, the individual or team that performed the change must create and submit a CR for review. Unauthorized changes must contain the same information as any other CR; the requirements are no different. The Unauthorized checkbox should be checked in order to identify the CR as unauthorized. Once the CR is reviewed and has been determined to meet all criteria for a Standard CR, the CM team will set the CCB Decision to CM Reviewed. This Decision indicates that the CR has been reviewed, but cannot be given an approval because it was unauthorized.
- **Caused Incident/Outage?** – If the implementation of the change(s) caused a new incident or outage it should be documented using this field. Make sure to document in detail the events that occurred.

- **Planning Issues?** – If the implementation failure was due to improper planning, we need to update this field and notes to the “Planning Issues Notes” text field. We may not always know if this is the case. If you learn it was a planning issue it is appropriate to document this here.
- **Follow-up Needed?** Field – used to document events after the fact. This is used for events such as validation results, test results or other items that were not and could not be available for CCB review. During the review of the CR you may identify items that you know are needed or the initiator has documented an event document is pending.

  NOTE: It is important to mark this field and document with what is pending so we can go back and review the CR for completeness. If the documentation is still missing the validation artifact contact the initiator and request a copy.

Release Info Tab



Change : "1984" (1 search records) (x) clear

Change: 1984 (Draft)

Summary:

Priority: 3

Change Control Board Decision

Release Documentation

Implementation Plan?

Implementation Plan Details

Validation Plan (Y/N)

Validation Plan Details

Rollback Plan (Y/N)

Rollback Plan Details

Release Notes (Y/N)

Release Notes Details

This form is used to document the release information such as Implementation Plans, Rollback Plan and Validation Plan which are all required for the completion of a CR. Release notes are not required for all changes, but are required for new application releases or updates to applications. An exception for required documentation may be allowed when the software is owned by a third-party vendor that is unwilling to provide that documentation. In the event that the documentation is not available, the DPS contact responsible for coordinating the work with the vendor must document any missing release information and add it to the CR after implementation. The CR reviewer should indicate the need for follow-up by checking the "Follow Up Needed" checkbox on the App/Metrics tab and updating the "Additional Notes" field.

Acceptable responses are **Yes** or **No**. If "**No"** is selected, a justification must be provided in the text box indicating why the documentation is not provided. If the response is "**Yes"**, review all provided information on the Release Info tab. The initiator can list the plans in the box provided, add links to external documentation stored in an approved repository, or attach them in the CR using the Attachment tab. Access each plan to verify if the correct documents are attached or linked.

- **Rollback Plan** (mandatory) – All CRs should document the rollback plan.

- **Implementation Plan** (mandatory) – The steps for implementing the changes on the CR should be listed here. This is a mandatory field and if blank or if the information is not clear, contact the Initiator and ask that this be added to the CR. Review the CR to ensure the plan is described or attached. If it is attached, validate the attachment.

An Implementation Plan is not just specifying who will perform the work, but actually **how** the implementation is being done in detail.

- **Validation Plan** (mandatory) – An explanation of how the changes will be validated should be included on all CRs. This field should explain how the change will be verified. If possible, before/after screen screenshots can serve as verification which can be attached to the CR. This can be explained to the initiator if needed.
  When the validation plan indicates screenshots will be provided after the implementation, go to the App/Metrics tab and click on the "Follow-up Needed?" box and add the explanation in the "Additional Notes" text box.

- **Release Notes** – Release notes are not required for all changes, but are required for new application releases or updates to applications.

Attachment (*) Tab

The attachment tab is used to upload artifacts such as supporting files, e-mails, artifacts, validation screenshots, test results, URLs, or other types of notes. Users can attach the approval e-mails. In most cases, an attachment is not required but is helpful in the CR review process.

Open each of the documents stored in this area and verify they contain relevant information.

***Note**: In the case when the CR requires User Action, a user notification is required to be attached to the CR.

Activity History (0) Tab

The Activity History tab tracks email activity related to a CR, which is usually initiated by business rules within the system. It also allows users to add notes to the CR or generate an email from the HEAT system.

Service, Risk Level, and Change Schedule Tabs

Not currently being used.

CR Monitoring

Once the review has been completed one of following actions should be taken:

Updating the Change Control Decision

Review Complete with no issues found

1. Update the Change Control Decision to "CCB Ready"
2. All CRs in "CCB Ready" will be reviewed by the CCB facilitator to familiarize (him/her) self with the CRs on the CCB agenda.

NOTE: If any additional issues are found during the review an e-mail will be sent to the CR Reviewer to send follow-up e-mail to the initiator/implementer to address the missing data. Follow the steps outlined under "Review Completed with issues" below.

Review Completed with issues

1. Update the Change Control Decision to "In CM Review Pending Update"
2. Send an e-mail to the in initiator/implementer asking them to update the CR with the missing data.
3. Monitor e-mails for responses and verify the changes have been made in HEAT.
    a. If the changes are complete
        i. Update Change Control Decision to "CCB Ready"
        ii. If no other follow-up items exist, remove the "Followup Needed?" checkbox. If validation artifacts are still pending, do not remove the checkbox.
    b. If the changes are not complete
        i. Follow-up with the initiator/implementer until all criteria have been satisfied or, if the changes are not completed before 2:00 pm on the day before CCB, send an e-mail reminder to all initiators with CRs still in "In CM Review Pending Update".
        ii. If the CR is not updated with the required information, inform the CCB facilitator via email of any outstanding issues.

Note: The ITSM team may return a CR to Draft status if it is not ready for presentation at CCB, based upon our review. This could result in the CR becoming a walk on, which requires the initiator to obtain approval from the appropriate DAD.

Reference material: CM_32_CR Emergency Approval

Changes to Approved CRs

How to handle changes to approved CRs is covered in the following document: CM-040_ITSM_Changing_Approved CRs.

Post-Implementation

CR Follow Up

1. Run the “CRs Req Follow-up” saved search a week or two after CCB to verify the validation artifacts have been added. Contact the initiator if follow-up items are still missing. If all of the pending artifacts have been received remove the “Follow-up Needed?” check.

CRs Needing To Be Closed

1. Run the “CRs Need To Be Closed” saved search every Monday morning. This will provide a listing of all Change Requests that have been completed more than 24 business hours prior.
2. This list should be emailed to the initiators requesting the CR be updated and closed.
3. If no action has been taken within 24 hours following the email, a second email should be sent individually to those with outstanding CRs.
4. If no action is taken after one week, a third email should be sent to the individual with their manager in the CC line.

Document Revision

Change 10

Version 2.6.3, April 06, 2017
Changed the Tuesday deadline from noon to 2:30PM. Author: Susie Miller;

Change 9

Version 2.6.2, May 17, 2016
Updated schedule time section; added list of times to be avoided. Author: Susie Miller; Peer Review by Christina Hardin

Change 8

Version 2.6.1, May 12, 2016
Updated links to the new SharePoint ; Author: Christina Hardin; Peer Reviewed Susie Miller

Change 7

Version 2.6.0, September 28, 2015

Fixed links to documents for the move from governance to operations. Susie Miller; Peer Review

Change 6

Version 2.5.0, July 29, 2015

- Moved the line “Equipment decommissions (e.g., CR 9924).” To the “Allowed” section of the document. Susie Miller; Peer Review

Change 5

Version 2.4.0, July 16, 2015

Added information about OIC Bridge emergency calls and fixed hyperlink to CM-032 CR Emergency Approval. Susie Miller; Peer Review

Change 4

Version 2.3.0, June 25, 2015

Various changes made after review: Multiple IT Approvers, Multiple Business Approvers, Attachment Tab verbiage, fixed broken link. Rudy Torres; Peer Review:

Change 3

Version 2.2.0, June 25, 2015

Added *new user action needed* functionality to require user notification when user actions are needed. Susie Miller; Peer Review:

Change 2

Version 2.1.0, June 05, 2015

Updated FYI section and moved hardware decommission from allowed to not-allowed. Updated the Questionnaire tab to reflect changes in hardware decommission process, Updated Apps/Metrics tab to include information for Cyber Security device scan and added MorphoTrust to maintenance CR list; Susie Miller; Peer Review:

Change 1

Version 2.0.0, February 25, 2015

Document re-write Release; Susie Miller; Peer Review: Youssef Fakhreddine, Rudy Torres, David Wade

Change 0

Version 1.0.0, February 5, 2014
Initial Document Release; Author: Kati Elliott; Approved by Paul Urban

Pilot Change Requests and Release Management

Information Technology Service Management

Document Version Date:
22 May 2015

TABLE OF CONTENTS

Purpose

The purpose of this document is to define the processes and terms for projects to be allowed a pilot status in the production environment. Pilot status means that the new application and associated dependencies be done in the production environment.

Reference

CM-000 Change Management Policies and Procedures

Definition

A pilot is an activity planned as a test, trial or burn in time for a new application as a proof of concept or a plan to move into production. The ideal project pilot sits at the confluence of project size, project duration, project importance and the engagement of the business sponsor.

1. Project size – You don't want a pilot that requires more than a 3-5 member team due to coordinating work among that many can substantially slow you down.
2. Duration - Pilots work better with shorter durations, such as, about three to four months.
3. Project importance – The importance of the project must be communicated as unimportant projects won't get the necessary attention from the rest of the organization.
4. Business sponsor – Working with the business sponsor ensures a higher degree of success. An engaged business sponsor can help the team if it needs to push against entrenched business processes, departments, or individuals.

Benefits

1. Allows for lessons learned in early phases to be incorporated in final production release.
2. Allows for progress in the absence of a QA environment.
3. Allows for data to be collected to make informed decision in moving forward.
4. Provides buy-in for change.
5. Helps control learning curve.
6. Helps define business benefits upfront.
7. Helps set realistic expectations.
8. Allows for testing and fine-tuning against actual production hardware.
9. Provides early opportunity to experience business benefits.
10. Allows support staff opportunity to test outlined troubleshooting procedures and escalations.
11. Identifies potential gaps in documentation and the Application's Operation Support Manual.

Requirements

1. No QA, limited QA or non-standard QA environments
   If there is no QA environment, then the app is forced to be tested in a production environment. Using production for your testing only, is not recommended nor is it a best practice.

   Disclaimer: Pilots can be a positive way to test or vet a new technology before we invest. A proper risk assessment should be completed to ensure that current production systems and data security are not negatively impacted. Prior approval from the Security team is required before beginning any pilot that uses the Production system.

2. Get ITSM buy in on Pilot
3. Change Request (CR)
   a. Must be completely filled out.
   b. Release tagged in code management system and added to CR.
   c. Code freeze – You are to baseline the code that is released for the pilot. That is the purpose for the code management tag.
   d. Documentation needed
      i. Initial Release Notes
      ii. Implementation plan
      iii. Rollback plan
      iv. Basic test results
      v. Security Approval
   e. Expectation is you are ready to deploy.
   f. The CR is not a place holder.
4. DPS IT Change Control Board Approval
   a. Pilot CRs that are approved at DPS IT Change Control Board (CCB) are expected to be implemented within the week. From Wednesday AM (after CCB) to following Wednesday AM.
5. Pilot CRs follow the DPS IT Change/Release process with the following exceptions:
   a. Application Operations Manual is not required at pilot release time. The manual will be required on the CR used to move the Pilot to production.
   b. Server setup document is not required at pilot release time. The server setup will be required on the CR used to move the Pilot to production.
   c. Support and Application Operation's Manual signoff is not required at pilot release time. The Operation's Manual signoff will be required on the CR used to move the Pilot to production.
   d. QA signoff is not required at pilot release time. QA signoff will be required on the CR used to move the Pilot to production.
   e. Monitor setup of application is not required.
6. All support for Pilot releases is understood to be done by the development team for the length of the pilot, unless an exception is made by management.

7. Pilots are not meant to circumvent the DPS IT QA or Security. QA and Security must still be involved.
8. Pilots can be stopped at any time by management.
9. All pilot releases are to notify the OIC before they begin and when they are done, as per our DPS IT official release process and policy.

Pilot Production Release

When a Pilot is completed and ready to move to an application production release, the following are required:

1. A production change request submitted. This CR can be cloned from the original Pilot CR.
2. CR completely filled out.
3. Code freeze – Code management system tagged for release.
4. Testing is done or QA signoff is expected.
5. Documents required
    i. Approved and signoff from appropriate support areas for the Application Operation's Manual.
    ii. Implementation & Rollback plan – either in the CR description, attached to CR or a link to SharePoint artifact.
    iii. QA/Users/testing Validation plan and results – Can be attached to CR or a link to SharePoint artifact.
    iv. All server/VM setup/validation documentation – received from the server team.
    v. Release notes
    vi. Support/Trouble Shooting Guide (TSG)/Escalation support (This can be a part of the Operations Manual.
6. Monitor setup is required through at least one of the DPS IT approved monitoring tools
    i. Solar Winds Orion
    ii. GIF
    iii. WUG – This is being phased out and will be replaced by Orion.
7. Training is completed. (User/Support)
8. Customer approvals received.
9. All implementers have signed up for the release time and are able to do their part in the implementation according to the written plan.
10. Security scan has been completed through Cyber Security team.
11. Change Request Approved at the DPS IT Change Control Board.
12. Application Support Owners are clearly identified with contact information and escalation groups listed

13. A pilot ceases to be a pilot when the proof of concept is done, and we remove it, or we follow the DPS IT process for releasing the new application into production. A pilot ceases to be a pilot at its production release.

Failure to meet the above requirements could prevent a CR from being reviewed at the CCB. The expectations of the DPS IT Change Control Board attendees are that all changes that are reviewed are complete and ready to be implemented. There is no further work required. The DPS IT expectation is also that the QA environment will be built out by production release timeframe.

Document Revision History

Change 2
Version 1.1.0, May 22, 2015
Updated format to comply with CM documentation standards. Removed references to SDE, replaced ISO with Cyber Security, removed Alan Ferretti, ; *Author: Susie Miller*

Change 0
Version 1.0.0, July 27, 2010
Initial Document Release; *Author: Paul Urban*

CM-032 CR Emergency Approval Process

Information Technology Service Management

Document Version Date:
26 October 2016

Table of Contents

If you are viewing this document on-line, save time by clicking the page numbers in the Table of Contents. CTRL+HOME take you back to the beginning of the document.

Purpose

This document contains the Change Management process for approving change requests. It is intended to describe the current CR approval process which should be followed by ITSM Review team and Emergency Change Control Board.

References

CM-000 Change Management Policies and Procedures
CM-001 ITSM Emg Change Process Flowchart

Approving FYI CRs when Using an Automated Email Notification to the OIC

The ITSM CR approver/reviewer does the following:

1. Ensure the FYI CR has **Type** of **FYI.**

2. Ensure the **Status** is **Ready to Review**.

3. Ensure the CR has passed the CR Review and includes the following:

   A – Attach approvals
   C – Cyber scans (when required)
   T – Test results (If you can't please specify why)
   I – Implementation, validation, rollback plans
   O – Operation manuals or support guide (as needed)
   N – Notification to users (if the change has downtime or user impact)

Approving Emergency CRs when Using Automated Emails

Sending the "ECR Voting Request" Email

The ITSM CR approver/reviewer does the following:

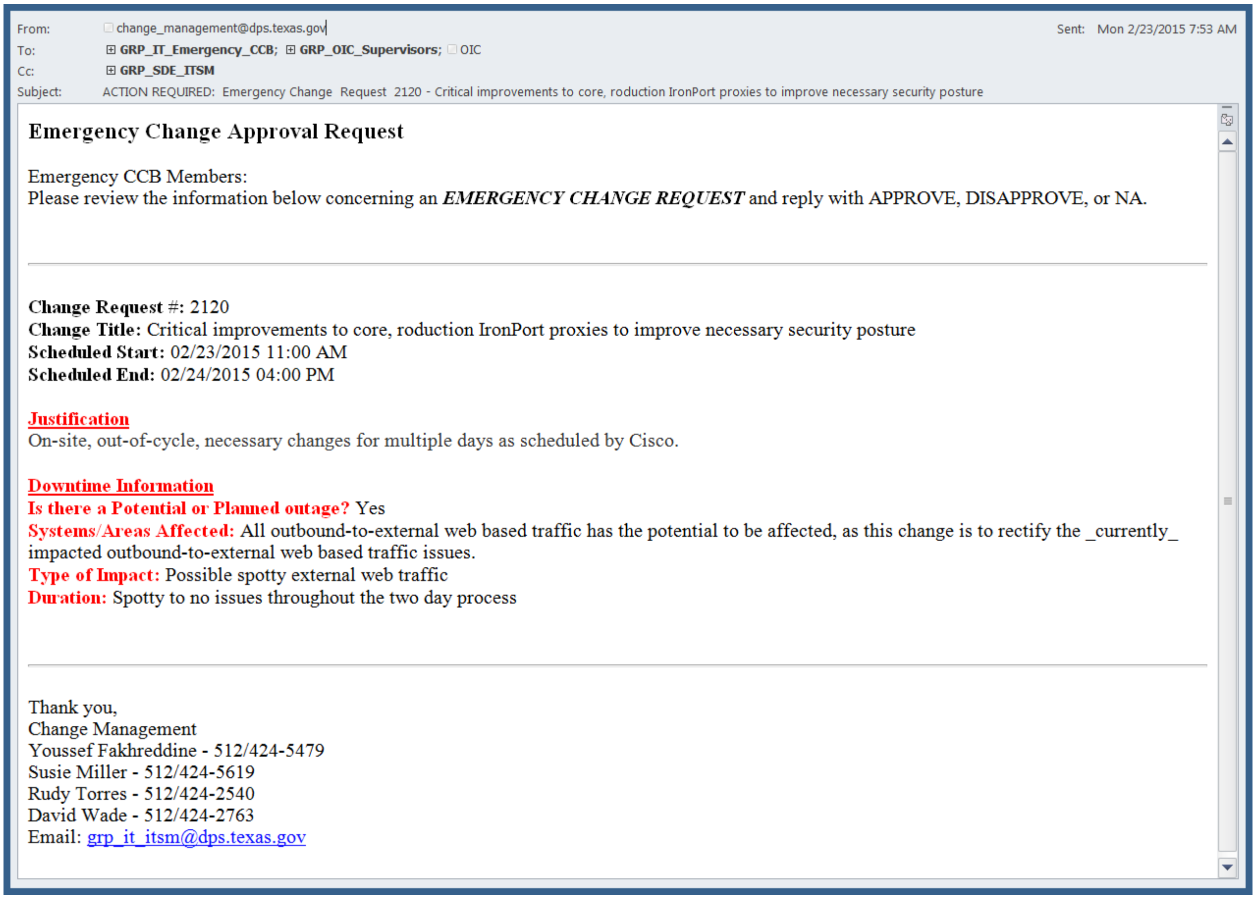
1. Ensure the Emergency CR has **Type** of **Emergency.**
2. Ensure the **Status** is **Ready to Review**.
3. Ensure the CR has passed the CR Review and includes the following:

   A – Attach approvals
   C – Cyber scans (when required)
   T – Test results (If you can't please specify why)
   I – Implementation, validation, rollback plans
   O – Operation manuals or support guide (as needed)
   N – Notification to users (if the change has downtime or user impact)

4. Update the **Change Control Board Decision** box to **Awaiting Emergency Approval.** Steps 1 and 2 must occur before this step. If you forget to do Step 1 or 2, perform 1 and 2 and repeat this step.

5. An email is automatically sent to the Emergency CCB and other appropriate recipients.

Sample “ECR Voting Request” Email



From: change_management@dps.texas.gov
Sent: Mon 2/23/2015 7:53 AM
To: ⊞ GRP_IT_Emergency_CCB; ⊞ GRP_OIC_Supervisors; OIC
Cc: ⊞ GRP_SDE_ITSM
Subject: ACTION REQUIRED: Emergency Change Request 2120 - Critical improvements to core, roduction IronPort proxies to improve necessary security posture

Emergency Change Approval Request

Emergency CCB Members:
Please review the information below concerning an ***EMERGENCY CHANGE REQUEST*** and reply with APPROVE, DISAPPROVE, or NA.

Change Request #: 2120
Change Title: Critical improvements to core, roduction IronPort proxies to improve necessary security posture
Scheduled Start: 02/23/2015 11:00 AM
Scheduled End: 02/24/2015 04:00 PM

Justification
On-site, out-of-cycle, necessary changes for multiple days as scheduled by Cisco.

Downtime Information
Is there a Potential or Planned outage? Yes
Systems/Areas Affected: All outbound-to-external web based traffic has the potential to be affected, as this change is to rectify the _currently_ impacted outbound-to-external web based traffic issues.
Type of Impact: Possible spotty external web traffic
Duration: Spotty to no issues throughout the two day process

Thank you,
Change Management
Youssef Fakhreddine - 512/424-5479
Susie Miller - 512/424-5619
Rudy Torres - 512/424-2540
David Wade - 512/424-2763
Email: grp_it_itsm@dps.texas.gov

Receiving the Votes

Before going to the next step, ensure that you have received a response from the members of Emergency Change Control Board with “Approved, Disapprove, NA” in the **IT_Change_Management** mailbox and that any objections have been mitigated. At any time, Executive Management can opt to override this policy when a more expedient approval is needed for an exceptionally urgent request.

Sending the “ECR Approval” Email

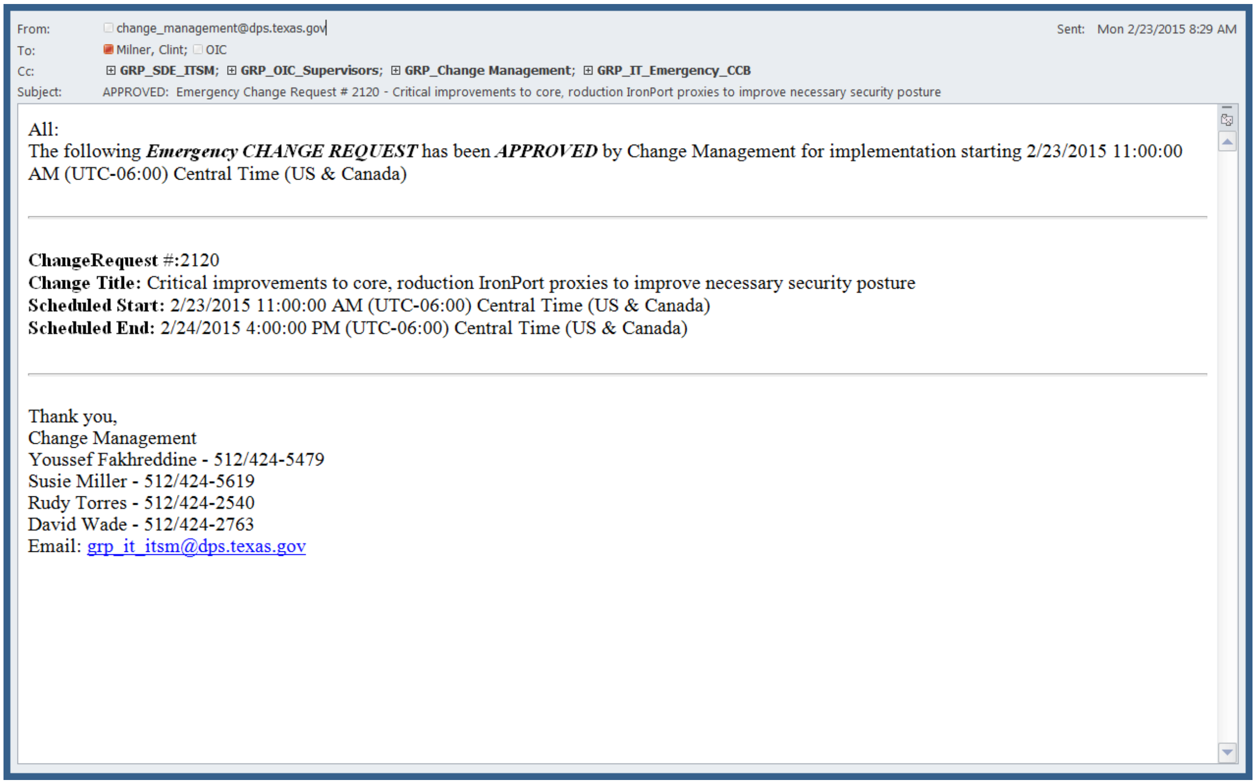
1. The Emergency Change Control Board members are responsible for reviewing and responding to Emergency Change Request Approval emails with “Approve”, “Disapprove” or “NA” within 2 hours.
2. In the event that a mission critical system is impacted, the allowed approval time will be shortened to 30 minutes and ECCB members will need to respond with “Approve”, “Disapprove” or “NA” within 30 minutes.
3. If a “Disapprove” response is received, the change will not receive final Change Management Coordinator approval until the concern is resolved and that ECCB member has provided approval.
4. All supporting documentation needs to be attached to the change request per Process Change # 1 above.
5. ***Having ensured that you have “Approval” in the IT_Change_Management mailbox and any objections have been mitigated***,
   revise the **Change Control Board Decision** box to **Approved.**

An email is automatically sent to the Emergency CCB and other appropriate recipients.

6. Click the CR’s save icon.

7. Exit the CR.

Sample “ECR Approval” Email



From: change_management@dps.texas.gov

Sent: Mon 2/23/2015 8:29 AM

To: Milner, Clint; OIC

Cc: ⊞ **GRP_SDE_ITSM**; ⊞ **GRP_OIC_Supervisors**; ⊞ **GRP_Change Management**; ⊞ **GRP_IT_Emergency_CCB**

Subject: APPROVED: Emergency Change Request # 2120 - Critical improvements to core, roduction IronPort proxies to improve necessary security posture

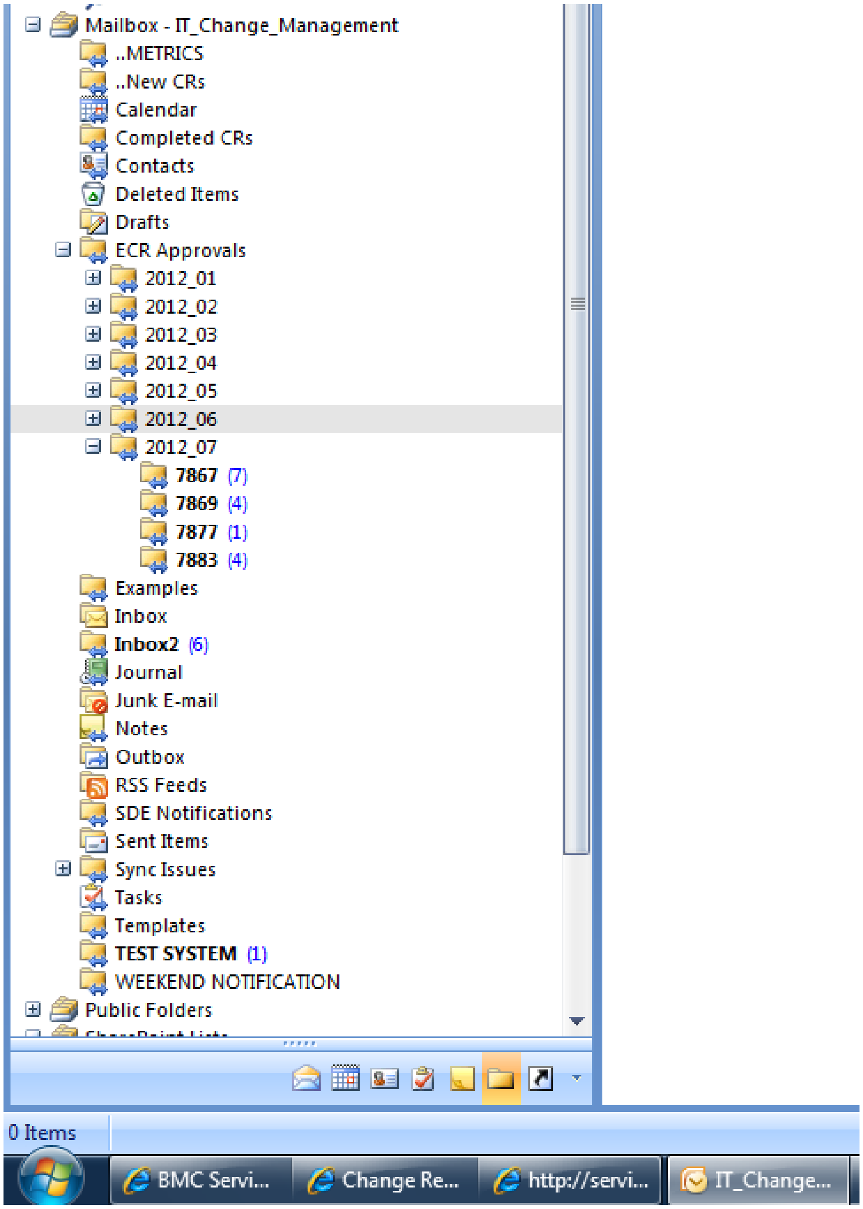
All:
The following ***Emergency CHANGE REQUEST*** has been ***APPROVED*** by Change Management for implementation starting 2/23/2015 11:00:00 AM (UTC-06:00) Central Time (US & Canada)

ChangeRequest #:2120
Change Title: Critical improvements to core, roduction IronPort proxies to improve necessary security posture
Scheduled Start: 2/23/2015 11:00:00 AM (UTC-06:00) Central Time (US & Canada)
Scheduled End: 2/24/2015 4:00:00 PM (UTC-06:00) Central Time (US & Canada)

Thank you,
Change Management
Youssef Fakhreddine - 512/424-5479
Susie Miller - 512/424-5619
Rudy Torres - 512/424-2540
David Wade - 512/424-2763
Email: grp_it_itsm@dps.texas.gov

Retaining the Voting Emails

Create an email folder named for the CR. This folder will reside in the **Mailbox IT_Change_Management** > **ECR Approvals** > ***yyyy_mm***



Drag and drop into this folder the related emails, including the “ECR Voting Request” email, the voting emails, and the “ECR Approval” email.

Document Revision History

Change 0
Version 1.0.0, July 27, 2012
Initial Document Release; *Author: Katheryn Wells*

Change 1
Version 1.1, February 25, 2015
Updated process to reflect current policies and updated definition of "sufficient approvals" for Emergency Change Requests.
Modified by: David Wade
Peer Reviewed by: Susie Miller; Rudy Torres

Change 2
Version 2.0, November 16, 2016
Updated process to reflect current policies for "approvals, disapprovals or NA" for Emergency change requests and ACTION items.
Modified by: Susie Miller

CM-040_ITSM_Changing Approved Change Requests

Information Technology Service Management

Document Version Date:
24 February 2016

TABLE OF CONTENTS

Purpose

The purpose of this document is to describe process for changing an approved Change Request.

References

CM-000_Change_Management_Policies_and_Procedures

CM-019 CR Review Process

CM-032 CR Approval

Procedures

Changing Approved CRs

Once a CR is approved, either by the CCB or by the Change Management team as authorized by the CCB, no changes should be made to it before implementation except in the following situations.

Schedule Changes

When unforeseen issues arise, planned start and planned end times may be rescheduled for change requests that have been approved but have not yet begun. In those cases, the initiator, assignee, or implementer is responsible for acquiring approval from the customers and IT managers and for seeking approval from the Change Management team (GRP_IT_ITSM@dps.texas.gov) who will verify that there are no conflicts with pre-existing CRs. Once the new schedule is approved, the Change Management team will notify the OIC and other appropriate parties of the change.
Note: If the rescheduled time falls within the next CCB cycle, the CR may need to be presented again.

If the change has already begun, only the planned end may be updated; the planned start may not be modified. Customers and managers must still approve, and Change Management must approve, update the CR, and notify the OIC and other appropriate parties as needed of the new schedule.

Change Management On-call schedule:
http://portal.tle.dps/sites/it/operations/itsm/SitePages/CM%20After%20Hours%20Schedule.aspx

Cancelling

If no work associated with the CR has occurred, and the clock has not yet started, approved CRs can be cancelled. The CR can also be returned to Draft status and resubmitted to CCB at a later date if the work is still expected to occur. In those cases, notify the Change Management team so the CCB decision can be updated.

If any work has occurred, the CR cannot be cancelled. It must be closed as rolled back, partially implemented, or implemented with issues, depending on how much of the implementation was performed. See Change Request Statuses for more information.

Altering Implementation Details

Once a CR has been approved, no implementation details should be modified or changed. If something in the implementation plan, validation plan, or possibly the rollback plan needs to be updated, contact the Change Management team. They will assist with determining if the details can be altered or if a new CR is required.
Note: If it is discovered after approval that other individuals or teams are needed, then the individuals and their managers must be notified prior to the start of the change to ensure that they are available. If not, the change may need to be rescheduled.

Closing

Change requests may remain open for up to one business day after completion. The initiator, assignee, or individuals implementing the change are responsible for updating the closing notes, adding any additional information or documentation that is required (e.g., post-implementation validation artifact), and closing the CR.
Note: The Change Management team will follow up on change requests that remain open past the one business day grace period.

Reopening

No one outside the ITSM team is able to reopen a closed CR. If the team determines that the CR does need to be reopened, then they will address the issue at that time. Contact the ITSM team (GRP_IT_ITSM@dps.texas.gov) if a closed CR needs to be modified.

Cancelled and closed change requests may not be reused. If an issue arises from a closed CR, a new one must be created and the previous CR identified in the new one.
Note: If needed, use the copy functionality in the Change Management System to create a similar CR.

Unauthorized Changes

An unauthorized change is a change made to a DPS system for which a change request (CR) should have been submitted and approved but was not. If a CR does not already exist for the change, the individual or team that performed the change must create and submit a CR for review. Unauthorized changes must contain the same information as any other CR; the requirements are no different.
Note: If ever unsure if work requires a change request, contact the Change Management team (GRP_IT_ITSM@dps.texas.gov).

Production Pilots

For information about production pilots, refer to the **CM-031_Pilot_Change_Requests_and_Release_Management** document on the ITSM SharePoint site: http://portal/sites/it/operations/itsm/documents/Documents/.

Change Request Statuses

The status in which a change request (CR) has been placed indicates where the CR currently is in the workflow and is indicated by the **Status** field on the CR form.

Open Statuses

While a CR is open, it is important to ensure it is in the correct status:

- **Draft** – The default status upon CR creation indicates that the CR is incomplete and is not ready to be reviewed by the Change Management team.
  Note: The Change Management team does not monitor or track changes in Draft status.

- **In Progress** – In Progress is set automatically once the OIC starts a CR.

- **On Hold** – The CR has been placed on hold by the initiator, assignee, OIC, and/or implementer. This is usually due to unexpected issues encountered prior to actual implementation. If the causes for the hold result in rescheduling, the Change Management team must be contacted first.

- **Ready to Review** – The CR is ready for the Change Management team to review for completeness.

- **Rollback-Open** – The CR was rolled back but remains open for rework within one business day.

Note: If the rework and corrections require more than one business day, the change should be closed and a new CR submitted when the change is ready to move forward.

Closed Statuses

When closing a CR, be sure to select the correct closing status.
Note: The Change Management team may reopen a closed CR and change the status if it is deemed necessary. A Post Implementation Results, also known as a Post Action Report, is a means of documenting the events that occurred during and after a change is implemented. A review and report is required under the following conditions:

- Change Rollback
- Change Implemented with Issues
- Change Partial Implemented
- Change Rollback – Open
- Change that caused an unknown/unexpected user impact, e.g., an incident (incident should be linked to the change)

- **Cancelled** – No work has occurred, and the CR has been cancelled.
- **Implemented With Issue** – The change was implemented but with unexpected results. If issues were encountered during implementation, the CR should be closed in this status even if the change was ultimately successful. Requires a PIR.
- **Partial Implementation** – Part, but not all, of the CR was implemented. Requires a PIR.
- **Rollback** – The change was rolled back, and the system, application, or item to be changed has been reverted to its state prior to any work occurring. This status will require a PIR.
- **Successful Implementation** – The entire CR was completed successfully with no unforeseen challenges or issues.

Document Revision

Change 0

Version 1.0.0, February 27, 2015

Added a section for reference materials; Susie Miller; peer review

Change 1

Version 1.1.0, February 24, 2016

Added a link to the Change Management On-call schedule; Susie Miller; Approved by Tony Cook 2/24/2016

Change 1

Version 2.0.0, October 19, 2016

Added information for PIR process; Susie Miller; Approved by Tony Cook 2/24/2016

Linking Incidents to Changes

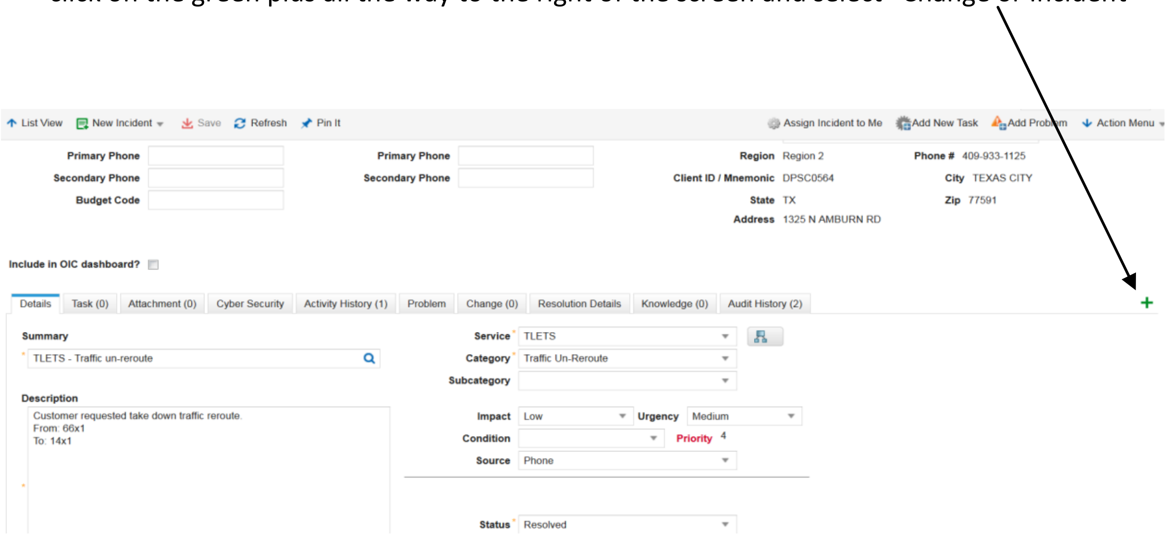
Information Technology Service Management

Document Version Date:
17 MAY 2016

Purpose

In an effort to understand the relationships between incidents and information technology changes within TXDPS, this document outlines how to link incidents and change requests within HEAT.

1. Adding the change request tab to an Incident or adding the Incident tab to a change request: click on the green plus all the way to the right of the screen and select "Change or Incident"



Primary Phone
Secondary Phone
Budget Code
Primary Phone
Secondary Phone
Region: Region 2
Client ID / Mnemonic: DPSC0564
State: TX
Address: 1325 N AMBURN RD
Phone #: 409-933-1125
City: TEXAS CITY
Zip: 77591

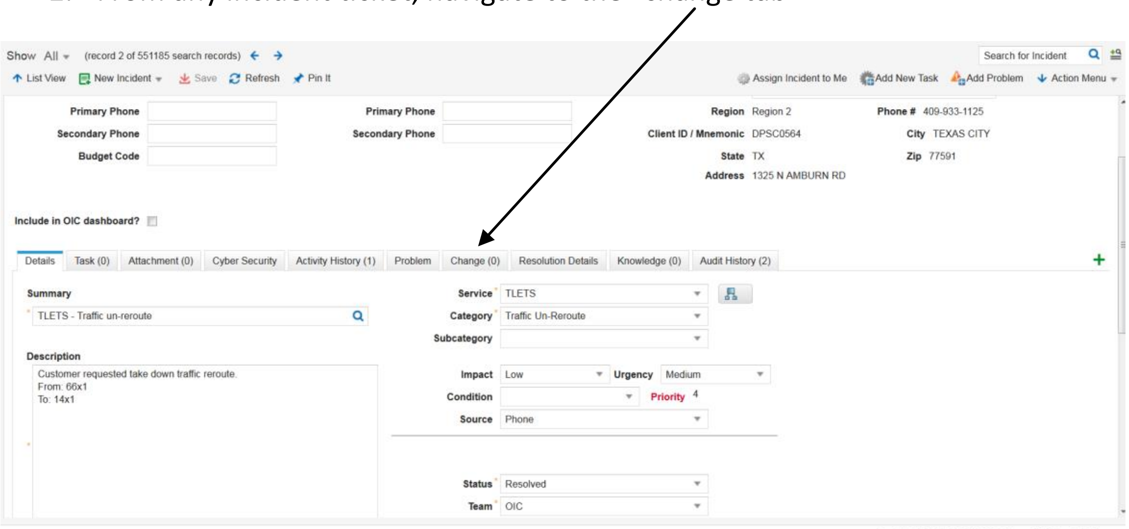
Include in OIC dashboard? □

Summary: TLETS - Traffic un-reroute

Description: Customer requested take down traffic reroute.
From: 66x1
To: 14x1

Service: TLETS
Category: Traffic Un-Reroute
Subcategory:
Impact: Low
Urgency: Medium
Condition:
Priority: 4
Source: Phone
Status: Resolved

2. From any incident ticket, navigate to the "change tab"



Primary Phone
Secondary Phone
Budget Code
Primary Phone
Secondary Phone
Region: Region 2
Client ID / Mnemonic: DPSC0564
State: TX
Address: 1325 N AMBURN RD
Phone #: 409-933-1125
City: TEXAS CITY
Zip: 77591

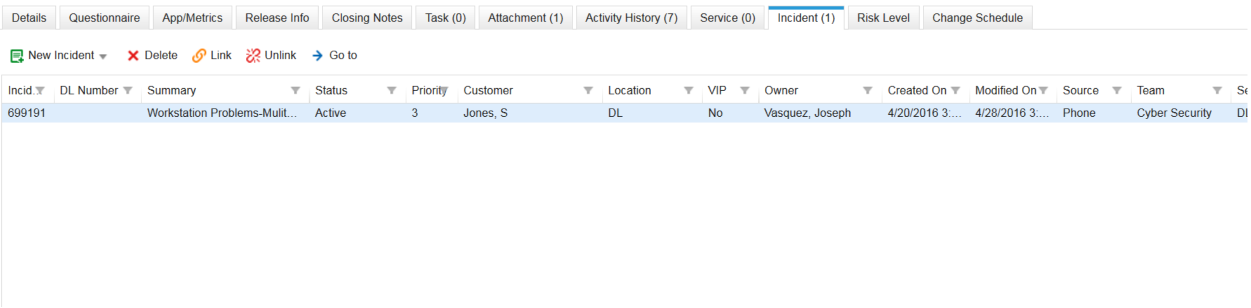
Include in OIC dashboard? □

Summary: TLETS - Traffic un-reroute

Description: Customer requested take down traffic reroute.
From: 66x1
To: 14x1

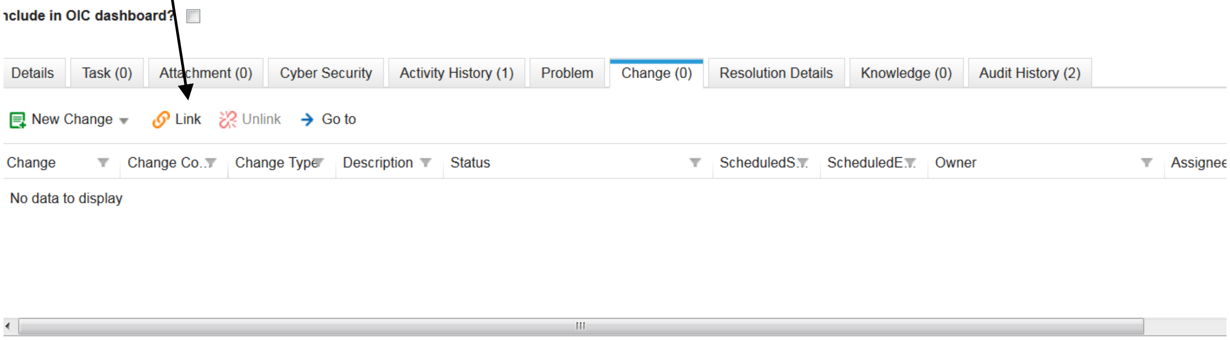
Service: TLETS
Category: Traffic Un-Reroute
Subcategory:
Impact: Low
Urgency: Medium
Condition:
Priority: 4
Source: Phone
Status: Resolved
Team: OIC

3. To link the record from a change request, select the “incident tab”



Incid	DL Number	Summary	Status	Priority	Customer	Location	VIP	Owner	Created On	Modified On	Source	Team	Se
699191		Workstation Problems-Mulit...	Active	3	Jones, S	DL	No	Vasquez, Joseph	4/20/2016 3:...	4/28/2016 3:...	Phone	Cyber Security	DI

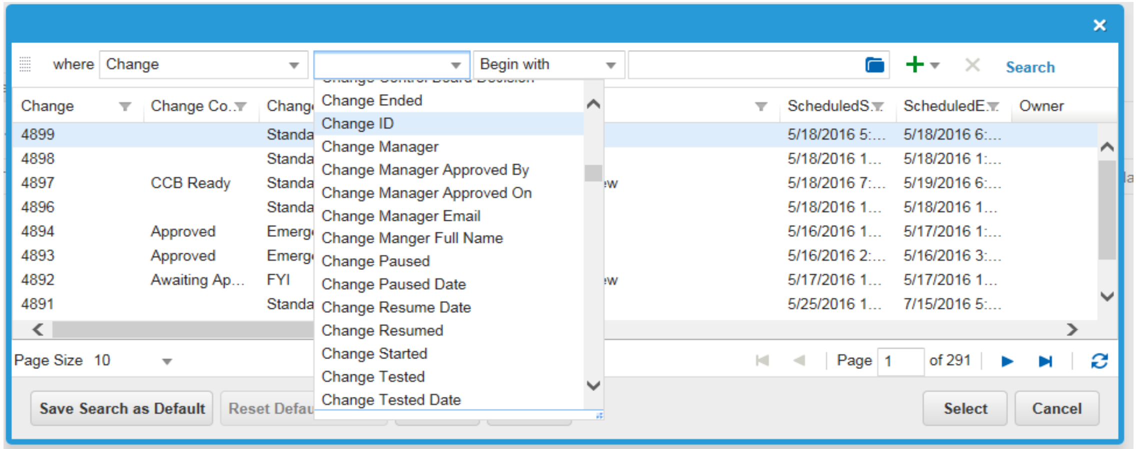
4. Select “link”


ıclude in OIC dashboard? ☐

Change	Change Co...	Change Type	Description	Status	ScheduledS...	ScheduledE...	Owner	Assignee

No data to display

5. You will need to select the following from the drop down menu: “ Change, Change ID, Equal to” then enter the CR #

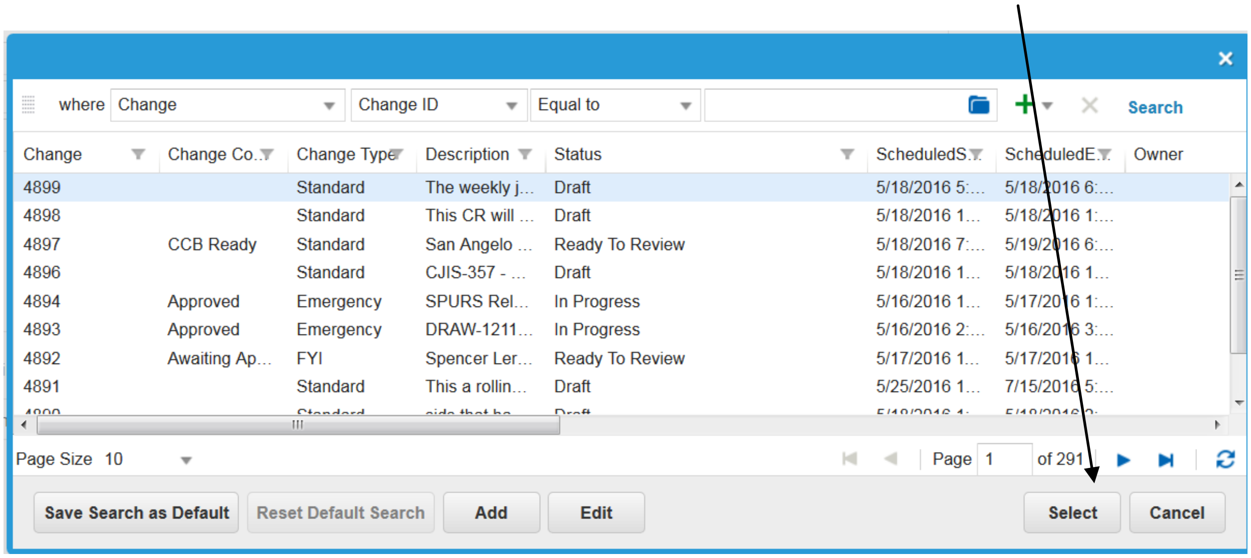

where Change | | Begin with

Change	Change Co...	Chang		ScheduledS...	ScheduledE...	Owner
4899		Standa		5/18/2016 5:...	5/18/2016 6:...	
4898		Standa		5/18/2016 1...	5/18/2016 1:...	
4897	CCB Ready	Standa	w	5/18/2016 7:...	5/19/2016 6:...	
4896		Standa		5/18/2016 1...	5/18/2016 1...	
4894	Approved	Emerg		5/16/2016 1...	5/17/2016 1:...	
4893	Approved	Emerg		5/16/2016 2:...	5/16/2016 3:...	
4892	Awaiting Ap...	FYI	w	5/17/2016 1...	5/17/2016 1...	
4891		Standa		5/25/2016 1...	7/15/2016 5:...	

Page Size 10

Page 1 of 291

6. Highlight the record that you want to link (change or incident) and click "Select". The screen shot below is an example of linking a change request to an incident record

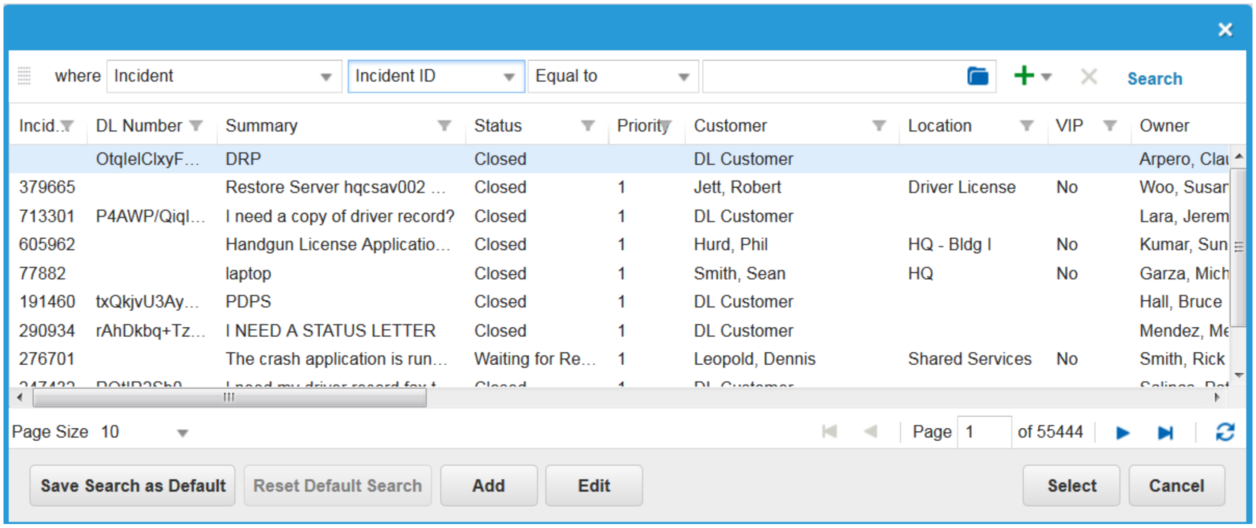


where Change | Change ID | Equal to

Change	Change Co…	Change Type	Description	Status	ScheduledS…	ScheduledE…	Owner
4899		Standard	The weekly j…	Draft	5/18/2016 5:…	5/18/2016 6:…	
4898		Standard	This CR will …	Draft	5/18/2016 1…	5/18/2016 1:…	
4897	CCB Ready	Standard	San Angelo …	Ready To Review	5/18/2016 7:…	5/19/2016 6:…	
4896		Standard	CJIS-357 - …	Draft	5/18/2016 1…	5/18/2016 1…	
4894	Approved	Emergency	SPURS Rel…	In Progress	5/16/2016 1…	5/17/2016 1:…	
4893	Approved	Emergency	DRAW-1211…	In Progress	5/16/2016 2:…	5/16/2016 3:…	
4892	Awaiting Ap…	FYI	Spencer Ler…	Ready To Review	5/17/2016 1…	5/17/2016 1…	
4891		Standard	This a rollin…	Draft	5/25/2016 1…	7/15/2016 5:…	

Page Size 10 | Page 1 of 291

7. Here is an example of linking an incident to a change request



where Incident | Incident ID | Equal to

Incid…	DL Number	Summary	Status	Priority	Customer	Location	VIP	Owner
	OtqlelClxyF…	DRP	Closed		DL Customer			Arpero, Clau
379665		Restore Server hqcsav002 …	Closed	1	Jett, Robert	Driver License	No	Woo, Susar
713301	P4AWP/Qiql…	I need a copy of driver record?	Closed	1	DL Customer			Lara, Jerem
605962		Handgun License Applicatio…	Closed	1	Hurd, Phil	HQ - Bldg I	No	Kumar, Sun
77882		laptop	Closed	1	Smith, Sean	HQ	No	Garza, Mich
191460	txQkjvU3Ay…	PDPS	Closed	1	DL Customer			Hall, Bruce
290934	rAhDkbq+Tz…	I NEED A STATUS LETTER	Closed	1	DL Customer			Mendez, Me
276701		The crash application is run…	Waiting for Re…	1	Leopold, Dennis	Shared Services	No	Smith, Rick

Page Size 10 | Page 1 of 55444

Document Revision

Change 0

Version 1.0.0, May 17, 2016

Initial Document Release; Author: Christina Hardin; Peer Reviewed by Susie Miller, Youssef Fahkreddine

Approved by Tony Cook

Post Implementation

Information Technology Service Management

Document Version Date:
12 October 2016

TABLE OF CONTENTS

Purpose

The purpose of this document is to outline the steps in completing a Post Implementaiton Results (PIR) and documentation requirements.

The initiator or implementer of the Change Request (CR) is responsible for coordinating a Post Implementation Results (PIR) on Changes with the following conditions: created an unknown/unexpected impact; a change that failed; a change with further impact than indicated from the review process; any lessons learned from change's should be documented through the Post Implementation Results (PIR) process.

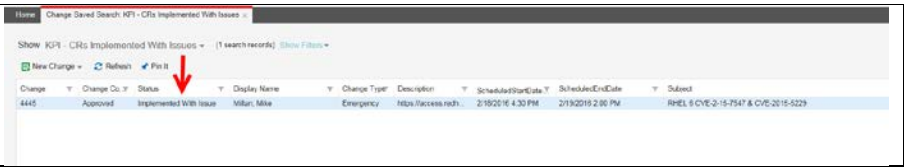
References

CM-000 Change Management Policies and Procedures
Change Request, CCB and CR Implementation Lifecycle Guide
CM-051 Linking Incidents to Changes

A Post Impelementation Results (PIR) also known as an After Action Report (AAR) is required under the following conditions:

- Rollback
- Implemented with Issues
- Partial Implementation
- Rollback – Open
- Changes that caused an unknown/unexpected user impact (incident should be linked to the change)

How to enter a PIR:

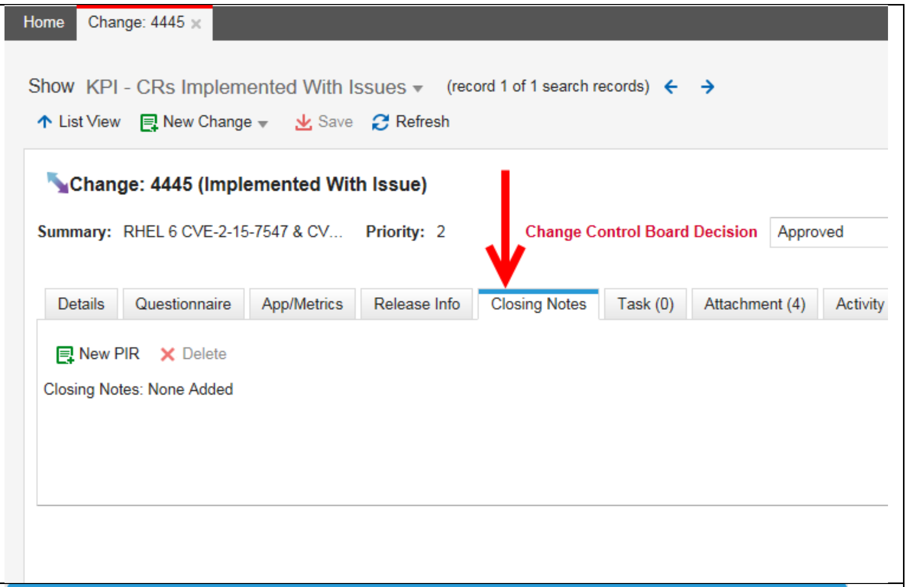
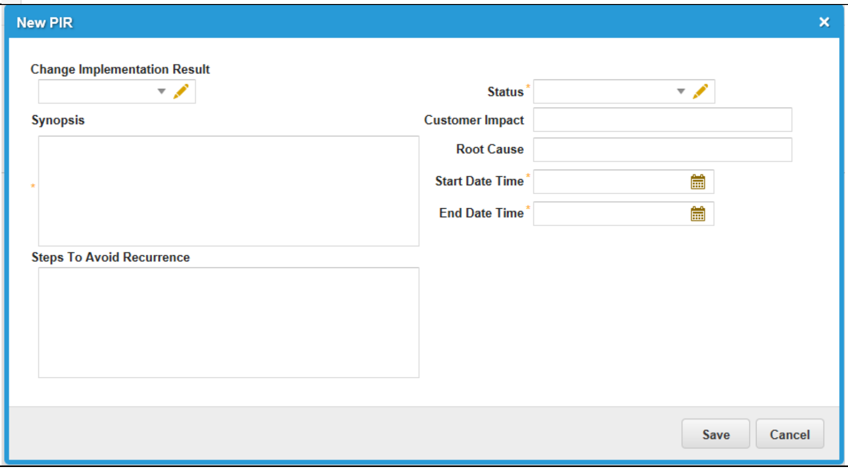
1.	Select the Change Request from the List View page	

Home | Change Saved Search: KPI - CRs Implemented With Issues

Show KPI - CRs Implemented With Issues (1 search records) Show Filters

New Change | Refresh | Pin It

Change	Change Co.	Status	Display Name	Change Type	Description	ScheduledStartDate	ScheduledEndDate	Subject
4445	Approved	Implemented With Issue	Millan, Mike	Emergency	https://access.redh...	2/18/2016 4:30 PM	2/19/2016 2:00 PM	RHEL 6 CVE-2-15-7547 & CVE-2015-5229

2.	Click on the Closing Notes tab	 Home · Change: 4445 × Show KPI - CRs Implemented With Issues (record 1 of 1 search records) List View · New Change · Save · Refresh **Change: 4445 (Implemented With Issue)** **Summary:** RHEL 6 CVE-2-15-7547 & CV... **Priority:** 2 · Change Control Board Decision: Approved Details · Questionnaire · App/Metrics · Release Info · Closing Notes · Task (0) · Attachment (4) · Activity New PIR · Delete Closing Notes: None Added
3.	Complete the PIR data fields then click on Save.	 New PIR × Change Implementation Result Synopsis Steps To Avoid Recurrence Status* Customer Impact Root Cause Start Date Time* End Date Time* Save · Cancel
4.		1.

NOTE: The PIR or AAR can be attached to the change request if additional documentation is needed.

Document Revision

Change 0

Version 1.2.0, October 12, 2016

Added a section for reference materials; Susie Miller; peer review

Change 0

Version 1.0.0, February 27, 2015

Added a section for reference materials; Susie Miller; peer review