NHS
West Hampshire
Clinical Commissioning Group

IT CHANGE MANAGEMENT POLICY

Version 5.2

Subject and version number of document:	IT Change Management Policy Version 5.2
Serial number:	COR/058/V5.02
Operative date:	1 October 2019
Author:	CSU Cyber Security Manager
CCG owner:	Senior Information Risk Owner
Links to other policies:	
Review date:	September 2021
For action by:	All Staff
Policy statement:	This document defines the policy for planning and managing the introduction of changes to IT services provided or hosted by South Central & West Commissioning Support Unit (SCW CSU)
Responsibility for dissemination to new staff:	Line managers at induction.
Mechanisms for dissemination:	All new and revised policies are promoted through the staff newsletter and intranet, and published on the CCG website.
Training implications:	All staff should be made aware of where to find CCG policies at induction.
Resource implications	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality analysis completed?	CSU equality impact assessment framework used to evaluate the policy (appended to policy).
Consultation process	CSU IT Senior Leadership Team CSU Corporate Governance Assurance Group CCG Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	11 September 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Jan 18	Cover	Review date extended to 25 May 2018 when GDPR enacted.	Jan 2018
2	Aug 18	Throughout	Complete review to bring in line with CSU approval process.	Aug 2018
3	Sept 19	Page 4	Updated re Head of IG role with SCW IG lead in section 8. Amend policy review from annual to biennial	Sept 2019
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
V5	Aug 18	CSU Cyber Security Manager	CSU IT Leadership Team CSU Corporate Governance Assurance Group CCG Policy Sub Group	See amend 2 above. Version control moved up to 5 (i.e. 2, 3 and 4 missed) to bring in line with CSU version control.
V5.2	Sept 19	As above	As above	See amend 3 above. Version control moved up to 5.2 in line with CSU version control.

IT SERVICES – CHANGE MANAGEMENT POLICY

As the South, Central & West Commissioning Support Unit (CSU) provides IT networks, equipment and support to West Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services core information security policies, in addition to those of the CCG.

The following policy was developed by the CSU IT Services Team and was adopted for use by the CCG. This has been identified as an IT Core Policy and as such cannot be amended by the CCG.

SUMMARY OF KEY POINTS TO NOTE

This document defines the Policy for planning and managing the introduction of changes to IT services provided or hosted by SCW CSU.

- The aim is to mitigate the associated risk and / or negative impact of change whilst responding to customers changing requirements
- There are three types of Change the definition of which will follow ITIL guidelines and are detailed within the Change Management Process document.
    - Standard Changes
    - Emergency Changes
    - Normal Changes
- All major and significant IT changes must be authorised by the Change Authorisation Board (CAB) comprising the IT Senior Leadership Team via a completed Request for Change (RFC)
- With the exception of Emergency Changes, all Changes that have an effect on the systems or services of IT Services customers must be communicated via the IT Service Delivery Team (or the SCW Communications Team if appropriate) with a minimum notice period of **5 working days** given to any sites and services affected by a Change
- For major or significant Changes further notice should be given. This notice will be agreed by the CAB members as part of the approval process and will be recorded within the Change.

OFFICIAL

IT Change Management Policy Version 5.2

South, Central and West Commissioning Support Unit
August 2019

DOCUMENT CONTROL

Document Name	Version	Status	Author
IT Change Management Policy	*5.2*	*Final*	*Change Manager*
Document objectives:	*This document defines the Policy for planning and managing the introduction of Changes to IT services provided or hosted by SCW.*		
Target audience:	*All staff*		
Committee/Group Consulted:	*SCW Information Governance Steering Group*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages*		
Approved and ratified by:	*SCW Information Governance Steering Group SCW Corporate Governance Assurance Group*	*Date: 19/08/2019*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*19/08/2019*		
Review date:	*July 2021*		
Author:	*Change Manager*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
	Arif Gulzar	1.0		Ratification from Corporate Governance Assurance Group
	Mike Dippie	2.0		Recommendations following review of existing Change Policy documentation – remove 'procedures' from the Policy. Standardise terminology. ITIL align wording. Removal of minimum votes process to avoid key stakeholders being bypassed. KPIs redefined to match wording in Policy Principles and Statement. Inclusion of PIRs Removal of the Director of IT Services from CAB
07/05/2017	Mike Dippie	2.1		Incorporating feedback from SW and DW
12/05/2017	Mike Dippie	2.2		Incorporating feedback from PW
08/06/2017	Mike Dippie	2		Inclusion of all approvals
22/06/2017	Mike Dippie	3.1		Add Richard Haynes to 'informed of' list
01/06/2018	Mike Dippie	4.1 draft		Annual review of Policy (including revised document format and updates to 'informed of' list
24/07/2018	Mike Dippie	5.0		Version changed after CGAG ratification
21/06/2019	Arif Gulzar	5.1	All	Policy reviewed and signed off by IT senior leadership team
12/07/2019	Arif Gulzar	5.2		Updated Head of IG role with SCW IG lead in section 8 as part of IG steering group approval feedback.
19/08/2019	Arif Gulzar	5.2	All	Policy ratified by SCW Corporate Governance & Assurance Group (CGAG)

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V5.1 21/06/2019
David Walch	Head of IT Service Delivery	V5.1 21/06/2019
Michael Knight	Associate Director of Technology Management and Architecture	V5.1 21/06/2019
Andy Ferrari	Associate Director of IT Strategy and Planning	V5.1 21/06/2019
Stephanie Wilson	Head of IT Services Development & Support	V5.1 21/06/2019
Cathy Jukes	Associate Director of IT Projects and Programmes	V5.1 21/06/2019

Contents

1. PURPOSE OF DOCUMENT

The objective of the Change Management process is to ensure that all Changes to IT services are assessed, approved, communicated, implemented and reviewed in a controlled manner. This approach will minimise the risk of disruption to South Central and West Commissioning Support Unit (SCW CSU) and its customers. It will ensure that affected customers are made aware of all Changes in advance of their implementation and have the ability to question them and even prevent them from taking place.

This document defines the Policy for planning and managing the introduction of Changes to IT services provided or hosted by SCW.

The aim is to mitigate the associated risk and / or negative impact of Change whilst responding to customers changing requirements.

The Policy provides the framework for the SCW IT Services Change Management Process; which must be followed by all SCW IT staff.
Relevant responsibilities of those involved are defined in the Change Management Process document.

2. SCOPE

Change is defined as 'the addition, modification, or removal of anything that could have an effect on IT Services'. This document sets out the Change Management policy within SCW IT Services. This policy covers IT systems, services and documentation used by SCW and its customers.

3. PRINCIPLES

The Change Management Policy is aligned to ITIL best practice guidelines.
IT Services provided to SCW customers which are subject to Service Level Agreements (SLAs) must be safeguarded.
In the event of a proposed Change being raised by the SCW or customer organisation, a full assessment and categorisation of impact, risk & probability must be undertaken prior to the Change being submitted.
Customer requester of the Change (i.e. which customer has requested and approved the Change) where appropriate will be clearly documented in each Change record.
All Changes to the "shared environment" supported by the SCW must be recorded in the Service Management tool.

The Process and Policy must be adhered to at all times for all:-

- Operational changes affecting the live environment.
- Test environment changes that have the potential to affect the live environment.

If there is any doubt as to whether an activity constitutes a Change, then guidance should be sought from the SCW Change and Release Manager.
Where the change requires a number of activities from different teams/individuals the Change Initiator is responsible for submitting and coordinating all aspects.

4. POLICY STATEMENT

The Change Management Policy is in place to control Changes to all critical and non-critical IT infrastructure and resources that underpin the day-to-day operations of the SCW and provides the Services to the customer as defined in their SLA.
Changes to systems will be managed and executed according to the formal Change Management process.
The control process will ensure that proposed Changes are reviewed, tested, authorised, implemented, communicated and released in a controlled manner; and that the status of each proposed Change is monitored to completion or retraction.
All documentation relating to any system or process will be updated to reflect any Changes.
No SCW employee is exempt from this policy and all third parties including customers who interact with the SCW must also comply.
A Post Implementation Review will be undertaken for all major Changes and any Changes which result in a major Incident.

5. TYPES OF CHANGE

There are three types of Change

- Standard Changes
- Emergency Changes
- Normal Changes

the definition of which will follow ITIL guidelines and are detailed within the Change Management Process document.

6. CHANGE CATEGORIES

The category of a Change is defined by its impact and risk. The category that is assigned will influence the level of authorisation required over the Change and the management input required throughout the implementation.

7. APPROVAL

All major and significant IT changes must be authorised by the Change Authorisation Board (CAB) comprising the IT Senior Leadership Team via a completed Request for Change (RFC).

This authorisation will:

- Provide assurance that it is a desirable Change
- That it does not conflict with other proposed Changes
- That a suitable and documented plan is in place
- A roll back plan is prepared and tested
- That all affected systems, services and end users have been identified and given sufficient notice
- That any relevant or interested third parties have been informed,

This assurance process will take place as part of the authorisation stage and will be documented.
The Change will be submitted, updated and approved or rejected via the IT Service Management Tool.
The Approval Groups for the different Change categories are detailed within the Change Management Process and must be adhered to (e.g. all major Changes must be formally approved by the 'Heads Of' (or designated Deputy) of **every** team within IT Services, as a minimum – additional approval may be requested at the discretion of 'Heads Of' or Change Management; Corporate Governance assurance group will be consulted as appropriate.
NB Change Management is responsible for identifying patterns in non-standard changes and recommending where these may become standard changes.

8. COMMUNICATION

With the exception of Emergency Changes, all Changes that have an effect on the systems or services of IT Services customers must be communicated via the IT Service Delivery Team (or the SCW Communications Team if appropriate) with a minimum notice period of **5 working days** given to any sites and services affected by a Change.

For major or significant Changes further notice should be given. This notice will be agreed by the CAB members as part of the approval process and will be recorded within the Change.
SCW IG Lead will be advised of any Changes which may have an impact on Information Governance and such Changes will also be communicated to the IG Steering Group.
Notification of a Change to a customer may result in revisions to the date of the change.
The Change notification must be in plain English and include a high level overview of the Change, with the option of further information being available if required.
Details of forthcoming Changes should be advertised on the relevant regional service desk portal and available to all customer staff.
Change communications must be checked for grammatical accuracy before issue.

9. COMPLIANCE AND MONITORING

Change Management will monitor the compliance of this Policy and any related documentation.
All documented processes will be kept under review and a report periodically made to the IT Services Senior Leadership Team and customer organisations.
Change Management will be responsible for the reporting functions of the Change process and will complete this in conjunction with all IT Services Teams.
Trend reports for Change will be communicated within the Change Management segment of the IT Service Development Group meeting.
The effectiveness of the Policy and Processes in meeting their purpose will be kept under review and reports submitted as required to the SCW IT Services Senior Leadership Team.
Failure to comply with the terms of SCW IT Change Management Policy and associated Process and governing policy could result in formal disciplinary proceedings lead by the appropriate Line Manager.

10. KEY PERFORMANCE INDICATORS

The following verification or audit measurements will be used to measure the overall effectiveness of the Change Management process:

Objective and Requirement	Example and Evidence (KPIs)
Changes to systems will be managed and executed according to the formal Change Management process.	% of Unauthorised Changes % of Emergency Changes
The control process will ensure that proposed Changes are reviewed, tested, authorised, implemented communicated and released in a controlled manner.	% of Change that have been correctly recorded, classified, assessed and actioned
A full assessment of categorisation of impact and risk must be undertaken. Prior to the Change being submitted.	% of Changes rejected at Assessment and Approval stage.
Minimise the adverse impact to customers	% of unplanned outages / major Incidents arising as a direct result of Changes % of Changes backed out

APPENDIX A CHANGE APPROVERS

Change Advisory Board (CAB) Members are drawn from the IT Services Senior Leadership Group (or authorised deputy*)

- Associate Director of IT Business Strategy and Planning
- Head of IT Service Delivery
- Enterprise Architecture
- Associate Director Of IT Led Programmes & Portfolio Management
- Associate Director of Technology Management
- Head of IT Service Development and Support

CAB requires authorised representation * from <u>all</u> ITS Teams – see above.

* Each Head of may appoint an authorised representative to Approve Changes when required.

Informed of all Changes but not Change Assessors or Approvers

- IT Business Planning Manager
- IT Business Relationship and Shared Service Manager
- IT Services Locality Senior Managers
- IT Services Portfolio Manager
- IT Services Senior Technical Programme Manager
- IT Services Senior Manager of System Operations
- IT Services Technical Programme Manager
- IT Services Incident Manager
- IT Service Delivery Operations Manager
- IT Services Problem Manager
- IT Service Level Performance Manager
- IT Services Sourcing & Contracts Manager

APPENDIX B CHANGE MANAGEMENT PROCESS

Change Management Process

Change Management Process current.docx

Version Number: 5.1	Issue/approval date: TBC
Status: Final	Next review date: July 2021

Appendix B

NHS
South, Central and West
Commissioning Support Unit

NHS South, Central and West Commissioning Support Unit

IT Services

Change Management Process

Author: Mike Dippie

Appendix B

Process	NHS South, Central and West Commissioning Support Unit, IT Services, Change Management Process
Version	3.1.
Status	Draft
Date	11/08/2017
Author	Mike Dippie

Reviewers	
Name	**Role**
David Walch	Head Of IT Service Delivery
Phill Wade	Associate Director Of Technology Management
Andy Ferrari	Associate Director Of IT Business Strategy and Planning
Stephanie Wilson	Head Of IT Services Development & Support
Cathy Jukes	Associate Director Of IT Led Programmes & Portfolio Management
Matthew Rawles	Enterprise Architect
Chris Borman	Senior Manager, Database of Operations 13/04/2017

Approvals		
Name	**Role**	**Approval Date**
Philip Evans	Director, IT Services	06/06/2017
David Walch	Head Of IT Service Delivery	02/06/2017
Phill Wade	Associate Director Of Technology Management – Deputy Chris Borman	06/06/2017
Stephanie Wilson	Head Of IT Services Development & Support	06/06/2017
Cathy Jukes	Associate Director Of IT Led Programmes & Portfolio Management	07/06/2017

Copies to ITS Services staff (as appropriate) via Team Managers

Document Versions				
Version	**Status**	**Author**	**Date of Issue**	**Comments**
0.1	Draft	Charles Allen	15:08:2016	
1.2	Draft	Charles Allen	23:08:2016	
1.0	Draft	Arif Gulzar	23/08/2016	
2.0	Draft	Mike Dippie	13/04/2017	Recommendations following review of existing Change Management Policy and Process documentation.
2.1	Draft	Mike Dippie	19/04/2017	Incorporate feedback from David Walch
2.2.	Draft	Mike Dippie	19/04/2017	Update Checklists to reflect Cherwell
2.3	Draft	Mike Dippie	12/05/2017	Rebranded Change Notification template
2.4	Draft	Mike Dippie	05/06/2017	Updated Role Titles for SLT
3.0	Final	Mike Dippie	05/06/2017	Approval
3.1	Final	Mike Dippie	28/07/2017	Inclusion of Standard Change process
3.2	Final	Mike Dippie	03/05/2018	Addition of CAB Webex process

Contents

1. Purpose of document

This document defines the process to be followed for planning and managing Changes to IT Services provided or hosted by the South Central and West Commissioning Support Unit (SCW).

The process fully complies with the IT Services Change Management Policy.

The process must be followed by all SCW IT staff.

Relevant roles and responsibilities are defined in this document.

2. Scope

Change is defined as 'the addition, modification, or removal of anything that could have an effect on IT Services'. This document sets out the Change Management process within SCW IT Services. This process covers IT systems and services used by SCW and its customers.

3. Objectives

The objective of the Change Management Process is to:-

- Control the lifecycle of all Changes, enabling Changes to be made with minimum disruption to IT services.
- Respond to customers changing business requirements while maximising value and reducing Incidents, disruption and re-work.
- Respond to customer and IT Requests for Change (RFC) that will align the services with the customer needs.
- Ensure that Changes are recorded and evaluated - and that authorised Changes are planned, tested, prioritised, documented, communicated, implemented, and reviewed in a controlled manner.
- Ensure that changes to Configuration Items (CIs) are recorded in the Configuration Management Database (CMDB).
- Optimise business risk – it is often correct to minimise business risk; but sometimes it is appropriate to knowingly accept a risk because of the potential benefit.

All SCW employees and 3rd parties involved in making changes to IT services are expected to comply with the process.

4. Types of Change

There are three types of Changes - Normal, Emergency and Standard.

Normal Change - any Change that is not a Standard or Emergency Change (see below) e.g. Firewall Changes, scheduled server reboots, routing changes, additions/removals/upgrades to applications/services, infrastructure moves.

Emergency Change – any Change that is urgently required to resolve or prevent a live incident e.g. the urgent reboot of a server or switch, applying an urgent security patch.

Standard Change - a pre-authorised Change that is low risk, relatively common and follows a procedure or work instruction. Examples of Standard Changes which are in scope of this document are :-

bulk data loads for a specific application (e.g. Business Intelligence)

software patching (although the patch needs to be tested before deployment)

minor firewall changes (i.e. to block an IP to address a security incident)

Other examples of 'Standard Changes' (e.g. creating new user accounts, password resets, PC/Printer installation, standard software installation) are currently out of scope of this document and should be submitted as Service Requests, following the Call Management Process.

5. Roles and Responsibilities

Stage	Change Initiator	Change Implementer	Customer	IT Services Teams	Service Delivery	Change Manager
6.1. Identify Change Control Required	R	C	CI	RC	RC	AC
6.2. Create RFC	R	CI		RCI	RCI	RAC
6.3. Assess RFC	CI	CI	CI	RC	RC	RAC
6.4. Pre-planning / update RFC	RA	CI		CI	CI	CI
6.5. Approval	RI	CI	CI	R	R	RA
6.6. Implementation	R	RA		CI	CI	CI
6.7. Verification	R	RA	CI	CI	CI	CI
6.8. Back Out (if required)	RCI	RA		RCI	RCI	C
6.9. Update RFC	RA	CI		CI	CI	CI
6.10. Communicate to customers	CI	RA	CI	CI	R	RCI
6.11. Update CMDB	RA	C		CI	CI	CI
6.12. Review / PIR	CI	CI		CI	CI	RAC
6.13. Close RFC	CI	I		I	I	RA
8. Reporting KPIs			CI	CI	CI	RA

RACI Matrix Key Responsibility Roles

R-Responsible

Those who do the work to achieve the task. There is typically one role with a participation type of *Responsible*, although others can be delegated to assist in the work required

A-Accountable

Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom *Responsible* is accountable. In other words, an *Accountable* must sign off (Approve) on work that *Responsible* provides. There must be only one *Accountable* specified for each task or deliverable.

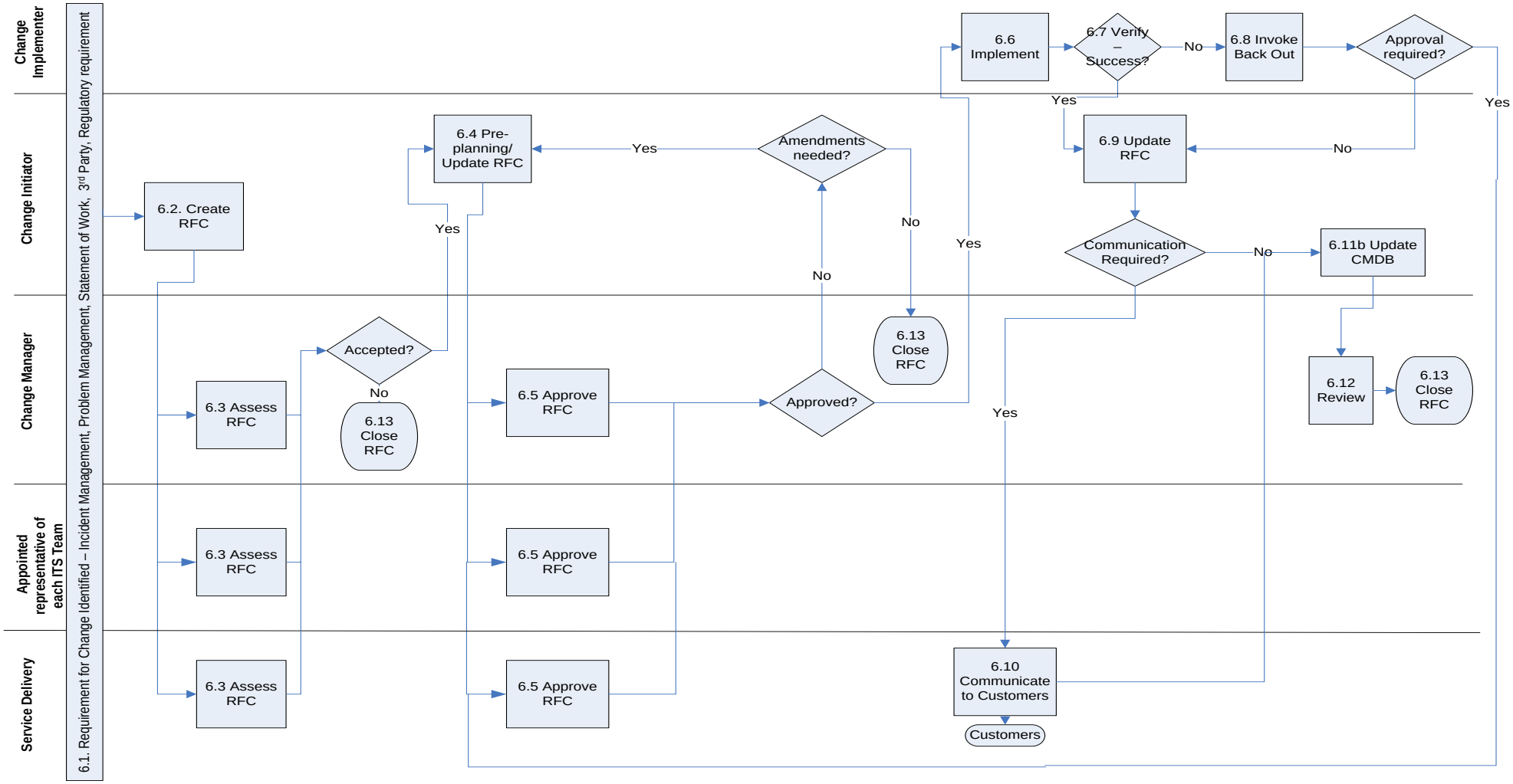
C-Consulted

Those whose opinions are sought; and with whom there is two-way communication.

I-Informed

Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

6. The Change Process



6.1 Identify the need for RFC

This need may arise from:-

- A Statement of Work item (at 'Delivery/Move' status) i.e. authorisation has been given to proceed with a work item
- Incident Management – to resolve an existing Incident or to proactively prevent an Incident occurring
- Problem Management – to address the cause of one or more existing or potential Incidents
- 3rd Parties (e.g. NHSE, EMIS etc) – third party notifies of amendments, additions or removals to hardware or software
- Regulatory requirements – e.g. to address a government requirement.

6.2 Create RFC

The Change should be raised by the Change Initiator as soon as the requirement for Change Control is identified.

Important note to Change Initiators - communication is the key to successful Change Management. Change Initiators should engage with impacted parties - IT Services staff and customers - as soon, and as clearly, as possible. Whilst Change Initiators are expected to update RFCs with all relevant information, the RFC is not the place for unnecessary debate or discussion to take place. If in doubt, contact relevant parties face-to-face, by phone or by email.

Planning Changes in this manner will reduce the chances of Changes being rejected or queried at Assessment and Approval stage; and support more effective utilisation of resources.

Mandatory fields are:-

- **Customer** – the person / organisation who is requesting the Change
- The **Reason for the Change**
- The **Service** that the Change will apply to
- The **Service Category**
- **Severity** – based upon the Impact and Risk
- **Title of request** – to assist, make this description concise and clear
- **Business Reason and Description** –including the impact of the Change (e.g. adding, amending or removing of CIs), Project Code / Cost Centre / Book of Work Reference (if applicable) or if the Change is to resolve or prevent any IT Incidents
- **Affected Systems** - what Configuration Items (CIs) and customers will be affected
- **Sites** – geographical locations impacted by the Change
- **Department** – any specific teams or departments impacted by the Change
- **Whether a Business Continuity Update/Documentation Request** is required
- **Implementation Date and time** - Ensure you refer to the Forward Schedule of Change (see Section 14 'Use of the Service Management tool') to minimise the chance of conflict with other Changes and allow a minimum of 5 days between distribution of any communications (which must be approved) and Change Implementation. See also Change Freezes

- **Anticipated outage**
- **Duration**
- **Risk and Impact Analysis** – include reasons why these assessments have been reached (e.g. this Change has been successfully tested on multiple platforms and piloted on user PCs)
- **Technical Analysis** – i.e. technical review sign off – this will usually be completed at a Team level to ensure proposed Change is technically and financially viable. This tab should also include:-
    - any Information Governance (IG) impact (if so, the Change Initiator will need to gain IG Approval)
    - any changes to maintenance or licensing arrangements
    - any changes to contracts/SLAs/OLAs
    - Any Customer impact – how each customer will be impacted, and any user involvement or training, timings of any outages required
    - Implementation Plan – including dates, times and resource requirements
    - Business Continuity – provide details of any impact on Business Continuity Plans; and confirmation that Business Continuity Manager has been informed.
    - Cyber Security - provide details of any impact on Cyber Security; and confirmation that Cyber Security Manager has been informed.
- **Communications Plan** – a base outline of any communications that may be required; including timescales for distribution. NB final communications will need to be agreed before the Change is Approved. NB Confirm the Service Desk are aware of the Change
- **Back Out Plan** - (including any go/no go points and timescales)
- **Acceptance criteria** – what checks will be made to ensure the Change has been successful and that there has been no adverse or unexpected impact
- Details of any related RFCs, Incidents or Problems.

Failure to provide sufficient mandatory information will result in the RFC not being approved. To assist Change Initiators, a checklist has been included at the back of this document.

6.3 Assess RFC

The purpose of this stage is for the Change to be initially Assessed by all 'impacted' IT Services Teams (each CI impacted by the Change will have an owner) – including any Teams that are required to work on the Change (i.e. to provide resource to implement and plan the Change) or support the CI being changed (e.g. IT Service Desk etc). Change Management will ensure that potential conflict with other Change activity is minimised by referring to the Forward Schedule of Change.

6.4 Preplanning

The Change Initiator needs to provide full details of the Change.

Mandatory fields are:-

- Customer sign off - including approval for the Change to be implemented by each impacted customer area (names, roles and date approval given)
- Test Plan - what pre-implementation testing has taken place (including who carried it out and the results of the testing).
- What post-implementation support is required and who will do it
- Post Implementation Evaluation Plan – what acceptance criteria needs to be met during the Verify stage of the Change – e.g. users can log on, performance is acceptable, functionality matches the customer requirements etc. Details of any customers who will be contacted to complete the evaluation, and when they will be contacted, will be required.
- Back Out Plan - (including any go/no go points and timescales)
- Access Requirements- details of any access required (e.g. datacentres/GP Practices)
- Immediate Support Plan - support following the Change (e.g. this might include a 'Warranty Period' where designated support arrangements have been made available specifically for the Change – e.g. floorwalkers)
- Business As Usual Support Plan - including advising Service Delivery how Incidents that may arise as a result of the Change will be handled, any training needed for support staff etc.
- Worst Case Scenario - if the Change was to fail what is the worst case scenario? Provide an estimate of how many users would be affected, how they would be affected and for how long (e.g. 600 users unable to access shared drive for 2 hours) and the Incident Severity that could result – see Incident Management Process
- Communication Plan – what information needs to be provided to customers and IT staff (e.g. advanced warning of outages, changes to customer environment, training guides etc). Who will issue the communication? When the communications needs to be issued. Who do the communications need to be issued to. See Communication Plan Process.

Failure to provide sufficient mandatory information will result in the RFC not being approved.

6.5 Approval

Approval must be given by **all** impacted IT Services Teams; including Changes sent for approval to CAB.

The Approval Process will vary according to the Category of the RFC (see above).

If further discussion regarding a Change is required, a Webex CAB will be arranged and chaired by Change Management. Change Initiators (or designated deputy) for the relevant Change will be required to be present to represent their Change. Failure to arrange suitable representation will result in the Change being rejected. Change Management will arbitrate a final decision to the agreement of impacted Teams.

NB consideration could be given to setting up a Group Mail Box for each Approving Team. This should ensure suitable coverage/deputisation in the event of the main Team Approver being unavailable (eg annual leave etc).

Major and Significant Changes – requires the Approval of CAB. CAB requires authorised representation from **all** ITS Teams, and Change Management i.e. the Head (or Deputies) of Strategy & Planning, TMO, Service Delivery, Service Development, Service Improvement and IT Led Projects & Programmes.

(Change Owners (or designated deputies) of Major or Significant Changes – which are at the 'Approving' stage of the Change lifecycle - must attend the next CAB to represent their Change(s).

Failure to do so may result in your Change not being Approved.

Minor Changes – require approval by representatives of **all impacted** ITS Teams and Change Management. All non-impacted ITS Teams will receive notification of Minor Changes via the Forward Schedule of Changes and have the authority to challenge the Approval of a RFC via Change Management.

Emergency Changes (can be either Major, Significant or Minor Changes) – these should be notified to Change Management as soon as the requirement for the Change is identified. Approval will be as above; but fast tracked in line with the urgency to implement the Change.

6.5.1. Change Approvers (CAB)

Change Advisory Board (CAB) Members are drawn from the IT Services Senior Leadership Group (or authorised deputy*)

- Associate Director of IT Strategy and Planning
- Head of IT Service Delivery
- Head of IT Enterprise Architecture & Design
- Associate Director of IT Projects and Programmes
- Associate Director of Technology Management & Operations
- Head of Service Development and Support

CAB requires authorised representation * from all ITS Teams – see above.

* Each Team Head may appoint an authorised representative to Approve Changes when required.

6.5.2. Informed of all Changes but not Change Assessors or Approvers

- IT Business Planning Manager

- IT Services Locality Senior Manager (B&NES, Gloucestershire, Swindon, Wiltshire)
- IT Services Locality Senior Manager (South region)
- IT Services Locality Manager (Thames Valley)
- IT Services Portfolio Manager

If necessary, a Change will be sent back to Change Initiator to make suitable amendments; and then re-submitted for Approval.

6.6 Implement

Once approved, the initiator may proceed with implementing the Change; taking into account any amendments instructed during the approval stage. The Implementation Plan (including 'go/no go' decision stages, communications and Back Out Plans) must be adhered to. Any proposed deviations from the Implementation Plan must be Authorised via Change Management. In the event that Change Management are unavailable (e.g. during 'out of hours'), the Initiator must gain approval from the ITS Leadership Team or by invoking the Out of Hours Support process if appropriate.

6.7 Verify

The Implementer verifies the success, or otherwise, of the Change using the Post Implementation Evaluation Plan.

6.8 Invoke Back Out Plan

If necessary, the Back Out Plan will be closely adhered to and invoked; including any Approval that might be required.

6.9 Update RFC

The Change Record will be updated by the Change Initiator to reflect the current status of the Change and any relevant comments regarding any unforeseen events during Implementation / Verification e.g. Back Out Plan invoked because users could not log on. NB it is important to document unexpected positive outcomes too, as these can be incorporated in Continuous Service Improvement initiatives.

6.10 Communication To Customers

Any communication regarding the success, or otherwise, of the Change will be triggered by the Change Initiator and issued by Service Delivery after appropriate approval has been granted – see Communication flowchart.

An email notification Template has been created see 13. Change Notification Template

NB in the event of an Emergency Change or 'Out Of Hours' communication being required alternative resources may be utilised to issue the communication.

6.11 Update CMDB

The Change Initiator makes appropriate updates to the CMDB to reflect any changes made as a result of the Change.

6.12 Post Implementation Review

The purpose of the PIR is to determine if all deliverables were successfully achieved to identify and action any possible areas of improvement – i.e. Continuous Service Improvement.

Change Management will invoke a Post Implementation Review (PIR) for all major and significant Changes; and any Changes requested to be investigated by the Incident Management or Problem Management process.

Change Management will identify and gain representation from all key stakeholders in the PIR process. A formal PIR Report will be distributed to Heads of (or designated Deputy) of Strategy & Planning, TMO, Service Delivery, Service Development, Service Improvement and IT Led Projects & Programmes plus the IT Service Incident Manager and IT Services Problem Manager.

NB the Change Management Post Implementation Review will **not** normally be distributed to customers – they receive Impact Reports from the Incident and/or Problem Management.

6.13 Close

Change Management will include any relevant information arising from the Change Review (e.g. PIR Minutes etc) and will close the RFC with one of the following success indicators:-

Failed, Implemented, Not Implemented, Rolled Back. It is recommended that the following Categories are used to assist in clarifying the outcome of a Change (eg the current process does not clearly differentiate between 'failed' 'not implemented' and' rolled back')

Disruptive (this needs to added to Cherwell) - Where the Change was implemented but there has been an outage or negative impact experienced by customers.

Rolled back - Where the change was successfully backed out without causing a disruption to customers.

Implemented - Change implemented and tested successfully.

Cancelled - (this needs to added to Cherwell) Where the change was not attempted at all e.g. the requirement for the Change is no longer necessary.

Rejected – (this needs to added to Cherwell) Where the change has been rejected by Change Management.

7. Standard Changes

This section defines the process to be followed for planning and managing Standard Changes – see Standard Change definition in Section 4.

7.1. Creating a Standard Change

- Change Owner submits Change for Approval as Standard Change by raising Normal Change (NB this can be an example of a previously implemented Normal Change); including any required Communication Plan.
- Request for creation of Standard Change is Approved or Denied.
- If Denied, Change Owner is notified and all subsequent changes of this nature are raised as a Normal change.
- If Approved - Change Owner creates Standard Change in Cherwell – including frequency of Changes.
- Change Manager creates new folder for the Change in shared drive O:\BSS\IT\Shared Area\Change Management\Standard Changes and advises Change Owner of its name.
- Change Manager amends Change in Cherwell to 'Standard'; with Scheduled End Date 3 months in advance (for review of Change to ensure it still meets Standard Change criteria) and attaches link to the Log of standard Changes
- Change Manager will distribute the list of Active Standard Changes with the 'Active RFC Report'.

7.2. Updating the Standard Change

- When Change Owner receives notification of updates for the Standard Change they will email details to the Change Manager.
- Change Manager will add the notification to the folder in the shared drive.
- Any communications and notifications of the update will be completed following instructions contained within the Standard Change.
- Change Manager will update the Scheduled Go Live Date in Cherwell – this will be visible in the Active Standard Changes Report.

7.3. Ongoing management of the Standard Change

- The Change Owner must notify the Change Manager of any amendments to the Standard Change e.g. change of frequency, additions to communications plan.
- The Change Manager will review these amendments and ensure that appropriate actions are taken; referring to the Change Management Policy and Process.
- Any standard change which causes an unexpected outcome or Incident will immediately be subject to a review by the Change Manager regarding it's suitability to remain as a Standard Change. If appropriate, subsequent Changes will be treated as Normal Changes.

8. Review of Change Process

8.1 The Change Manager will carry out ongoing reviews of the performance of Standard Changes - in conjunction with the Incident and Problem Managers- ensuring no adverse effects have occurred, identifying any opportunities for Continuous Service Improvements; and take appropriate actions.

8.2 All Standard Change will be reviewed after an initial period of 3 months; increasing to 6 months thereafter.

9. Change Freezes

A Change Freeze is a restriction on the Implementation of Changes usually to protect the customer environment during critical activity (e.g. financial year end) or where limited resources are available to support Changes (e.g. Christmas/New Year). In reality, there will be occasions when Changes are required during a Change Freeze. In this event, due diligence should be applied to mitigate any additional risks.

10. Key Performance Indicators

How the process will be measured to ensure it is effective and efficient.

Objective and Requirement	Example and Evidence (KPIs)
Changes to systems will be managed and executed according to the formal Change Management process.	% of Unauthorised Changes implemented % of Emergency Changes
The control process will ensure that proposed Changes are reviewed, tested, authorised, implemented communicated and released in a controlled manner.	% of Change that have been correctly recorded, classified, assessed and actioned
A full assessment of categorisation of impact and risk must be undertaken. Prior to the Change being submitted.	% of Changes rejected at Assessment and Approval stage.
Minimise the adverse impact to customers	% of unplanned outages / major Incidents arising as a direct result of Changes % of Changes backed out

11. Checklist for Change Initiators

Information Required – (see sections 4.2. and of Change Process 4.4. for more information)	Change stage that Information Required		Update Field or Tab in Change Record	Check
	Assessment	Approval		
Customer – the person/organisation requesting the Change	Mandatory	Mandatory	Home screen	
The reason for the change			Home screen	
The service that the Change applies to			Home screen	
The Service Category			Home screen	
Severity – based upon the Impact and Risk			Home screen	
Title of request			Home screen	
Business Reason and Description – including the impact of the Change (e.g. adding, amending or removing of CIs), any Project Codes etc or if the Change is to resolve or prevent any IT Incidents			Home screen	
IG Input Required - details of any IG impact and IG approval			Home screen	
Affected Systems - what (CIs) and customers will be impacted			Home screen	
Sites – geographical locations impacted by the Change			Home screen	
Department – as above			Home screen	
Implementation Date and time - Ensure you refer to the Forward Schedule of Change and allow a min 5 days between distribution of any communications and Change Implementation. See also Change Freezes			Home screen	
Any anticipated outage			Home screen	
Risk and Impact Analysis			Risk/Impact tab	
Technical Analysis – i.e. technical review sign off			Technical tab	
Back Out Plan - (including any go/no go points and timescales)			Backout tab	
Confirm the Service Desk are aware of the change			Comms tab	
Business Continuity – any impact on Business Continuity Plans			Technical tab	
Cyber Security – provide details of any impact			Technical tab	
Details of any related RFCs, Incidents or Problems.			Technical tab	
Any changes to maintenance or licensing arrangements			Technical tab	
Any changes to contracts/SLAs/OLAs, any outages required			Technical tab	
Customer impact – how each impacted CI will be impacted, and any user involvement or training, timings of any outages etc			Technical tab	
Draft Communications Plan – an outline of any communications that may be required; including timescales for distribution			Comms tab	
Implementation Plan (resource and contact details – include any third parties)			Technical tab	
Customer sign off - approval for the Change to be implemented by each impacted customer area (names, roles and date approval given)	Optional		Comms tab	
Test Plan - what pre-implementation testing has taken place (including who carried it out and the, results of the testing).			Technical tab	
Final implementation Plan			Technical tab	
Post Implementation Evaluation Plan – what acceptance criteria needs to be met during the Verify stage of the Change – e.g. users can log on, performance is acceptable, functionality matches the requirements			Acceptance Criteria tab	
Access Requirements - details of any access required			Technical tab	
Post implementation Support (immediately after the change)			Technical tab	
Business As Usual Support Plan - how Incidents are handled, document any training needed for support staff etc.			Technical tab	
Final Communication Plan – comms to customers and IT staff (e.g. advanced warning of outages, changes to customer environment, training guides). Who will issue the communications, who to and when it needs to be issued. See Communication Plan Process			Comms tab	

12. Timescales

The minimum time between a RFC being raised and a Change being implemented

Stage	Change Category			
	Emergency	Major	Significant	Minor
Raise RFC	asap	1 day	1 day	1 day
Assessment	asap	2 days	3 days	3 days
Pre-planning	asap	1 day	1 day	1 day
Approval	asap	5 days	2 days	2 days
Implementation	asap	1 day	1 day	1 day
Min time Between RFC Being Raised And Implementation Date *	**N/A**	**10 days**	**8 days**	**8 days**
Update CMDB		1 day	2 days	5 days
PIR		2 days	2 days	5 days

* **it is vital that sufficient time is allowed to issue any required communications to customers – usually a minimum of 5 working days – see Change Management Communication Process Flow**

13. Change Categories

Risk / Probability	Impact / Incident Priority in Worst Case Scenario		
	High (P1 Incident)	Medium (P2 Incident)	Low (P3 or P4 Incident)
High	**Major**	**Major**	**Significant**
Medium	**Major**	**Significant**	**Minor**
Low	**Significant**	**Minor**	**Minor**

NB Standard Changes are pre-Approved and therefore do not feature in the above matrix.

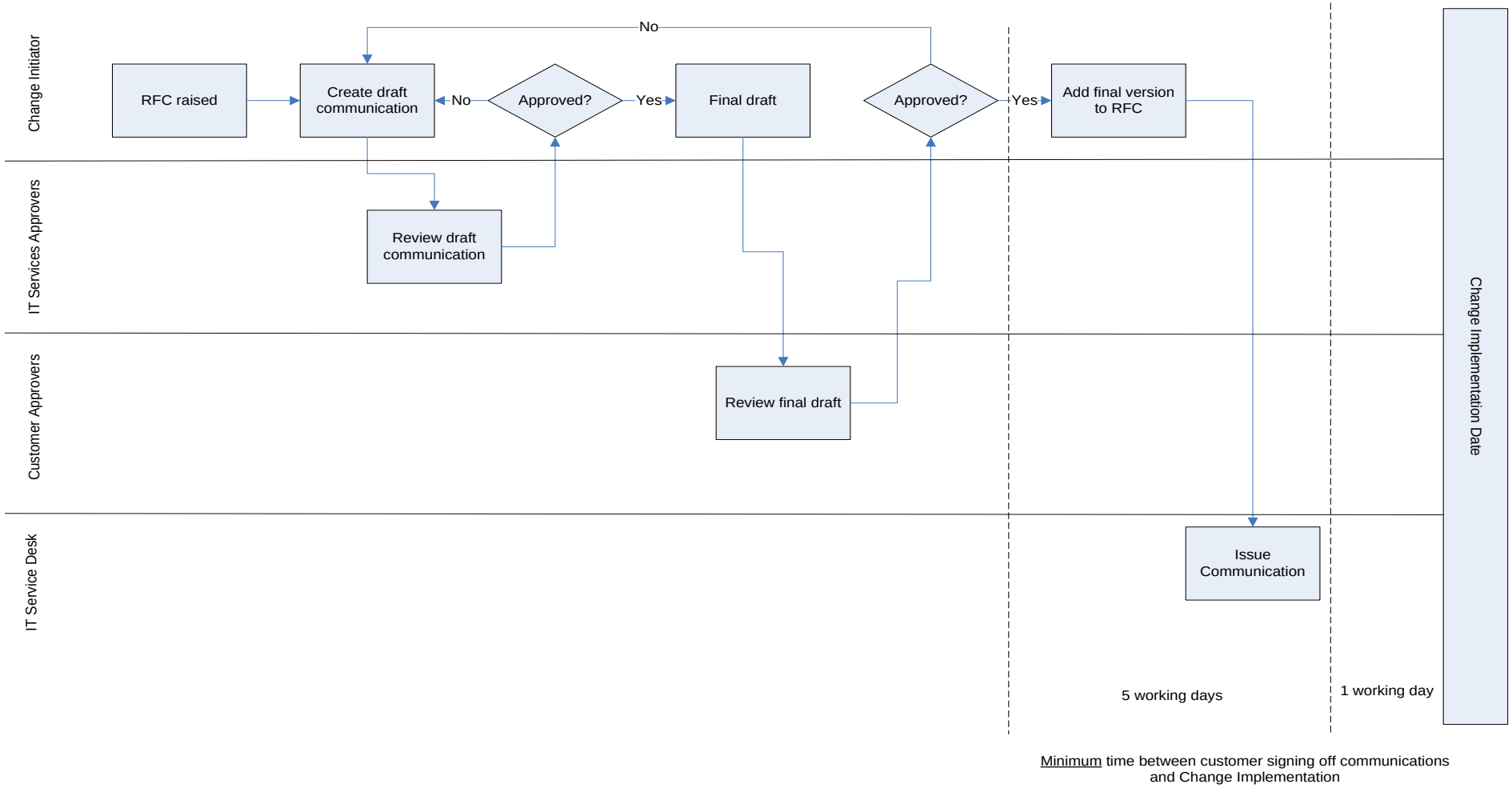
Risk / Probability

High – tried before with disruption, or never tried before and/or the system or infrastructure is currently in a poor state of repair and the likelihood of adverse impact on customers is significant or high

Medium - tried before but complex or tried before, or caused problems - but cause of problems should now be eliminated

Low – not tried before but simple or similar in nature to previous Changes

14. Communication Process Flow



15. Change Management Notification Template

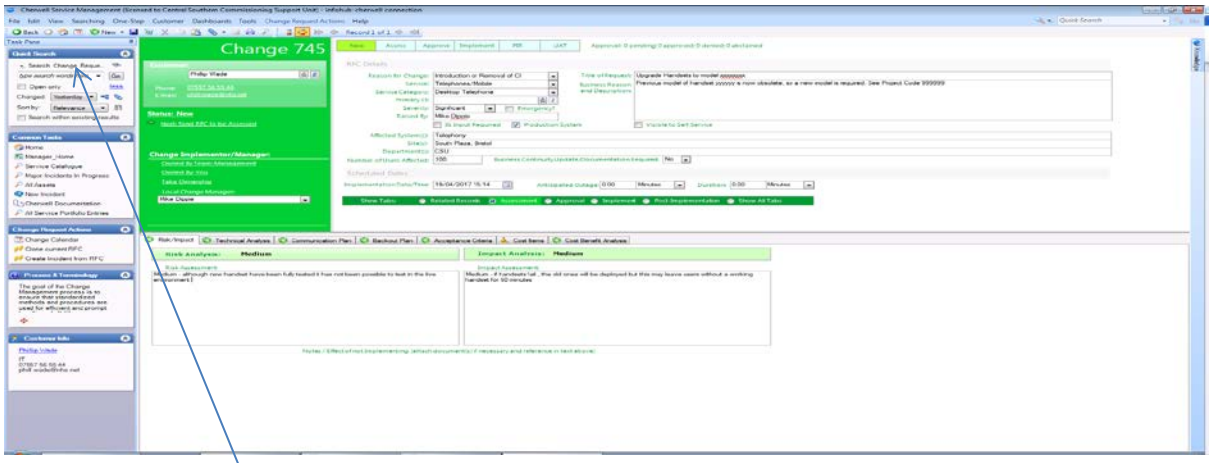
Click here for the latest version of the Change Notification template.

16. Use of the Service Management tool

Creating a Change Request

Log into Cherwell using your LAN ID and password, Click the File menu, Click the New menu, Click New Change Request

The screen below will be pre-populated with a Change Ref and your name in the Raised By field



Searching

Search for RFCs can be done by entering a valid Change number in the 'Quick Search' field or using the 'Search Change Request' option.

Completing the main screen

All the fields detailed in the Change Initiators Checklist must be completed before the Change is sent for assessment. For Customer Name enter their surname and then Enter. If the Customer Name is not identified in Cherwell the Change Initiator should use the relevant Customer Organisation/Practice Name – typically this will be in the format 'NHS XXX CCG' etc. If a new Organisation/Practice Name needs to be added, notify the Change Manager.

Completing the information tabs

All tabs - with the exception of Cost items and Cost Benefit Analysis - must be completed with relevant and accurate information. Once all the mandatory fields are completed the RFC should be saved. The RFC will then automatically move to Assessment.

Change Initiators should monitor the progress of any RFC they initiate and respond to any requests for additional information in a timely manner. Failure to do so could result in a RFC not being approved in time.

Forward Schedule of Change (FSC)

The FSC can be found in the current Service Management Tool by selecting Tools – Calendars – Change calendar.

Post-Approval updates

Once the RFC has passed the Approval stage, the Change Initiator should provide further updates in the Change Management tool regarding progress by updating the Implement and Post-Implementation tabs.

'Cloning' Changes

To create a clone RFC from a previous record (e.g. applying regular Microsoft updates to a server) – search for and highlight the previous record, and select Change Request Action (from the toolbar) and click 'Clone current RFC'.

Requesting access to the Service Management

Any members of staff who require access to the Service Management tool should submit a request to the IT Service Desk.

***** Document Ends *****

APPENDIX C EQUALITY IMPACT ANALYSIS

On the IT Change Management Policy

1 What is it about? ***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The IT Change Management Policy defines the policy for planning and managing the introduction of Changes to IT services provided or hosted by SCW.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? No impact
d) What are the barriers to meeting this potential? There are no barriers.
2 Who is using it? ***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy.
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.
3 Impact ***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? This is not applicable.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.

d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Stephanie Wilson**	Date completed: **23-07-2018** Proposed EIA review date: **01-07-2019**
Signature of director/decision-maker **Simon Sturgeon** Name of director/decision-maker **Simon Sturgeon**	Date signed **23-07-2018**