CHM1 Manage changes including emergency changes

Document control

Area	CHM
Procedure status	**FINALISED**
Owner	Matthew Viljoen
Approval status	**APPROVAL REQUESTED** ☐ Tiziana Ferrari ☐ Yannick Legre
Approved version and date	v. 70 27 Oct 2016
Statement	Procedure how a change should be registered, approved and reviewed after implementation.
Next procedure review	☐ 01 Feb 2017 Matthew Viljoen

Procedure reviews

The following table is updated after every review of this procedure.

Click here to expand...

Date	Review by	Summary of results	Follow-up actions / Comments

Table of contents

- Document control
- Procedure reviews
- Table of contents
- Overview
- Definitions
- Entities/roles involved in the procedure
- Triggers
- Normal change workflow
- Standard change workflow
- Emergency change workflow
- Workflow shown graphically
- Schedule of Changes
- Appendix A - Quality of change

Overview

This procedure describes the lifecycle of changes affecting (either directly or indirectly) services listed within the EGI Service Catalogue as well as the transition of all major changes and new services coming from SPM. This procedure includes registering, assessing, approving and reviewing Requests for Change (RFCs), in addition to managing pre-approved or 'standard' RFCs. Finally the procedure for managing emergency changes is covered.

The tool for managing the lifecycle of RFCs is EGI RT. This supports the entire lifecycle of change requests from registering to the historical

searching of RFCs.

The list of pre-approved or 'standard' RFCs for a service shall be created and maintained in the EGI Wiki. Its existence shall be made known to all operational staff for the service.

Regarding the UMD and CMD, EGI fulfils the role of a distributor of software and coordinator of the Staged Rollout activity to regulate the updating of software in a semi-controlled environment. With respect to Change Control, the updates are controlled and implemented by the Resource Centres (RC) themselves. EGI makes new software releases available in its UMD/CMD distributions, but this in itself does not trigger software updates of user-facing software, as a separate step is required to do this when the RCs choose to upgrade their software. This decision is made by the RCs and not by EGI. As such, EGI cannot control the execution of the changes in the way that it can of services listed within the EGI Service Catalogue. While EGI should encourage RCs to implement their own Change Control process (if they do not have them already), the upgrading of software from UMD/CMD is outside the scope of EGI CHM, with exception of unsupported Middleware at Resource Centres triggering procedure PROC01 EGI Infrastructure Oversight escalation.

Definitions

Please refer to the EGI Glossary for the definitions of the terms used in this procedure.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", “MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Emergency change - A Change that must be introduced as soon as possible to resolve a Major Incident or to implement a security patch.

Standard change - a Change that is a recurrent, well known change that has been proceduralized to follow a pre-defined, relatively risk-free path, and is the accepted response to a specific requirement or set of circumstances, where authority by the CAB is effectively given in advance of implementation.

Entities/roles involved in the procedure

Entity/role	Description
Change Owner	The person who is in charge of the change, wants it to happen and is following it through from initial planning to implementation and review. It is typically the Service Owner of the service which is affected by the change.
Change Implementer	The person who leads or coordinates the implementation of the change. This may be the same person as the Change Owner.
Service Owner	The person responsible for the service affected by the change or the line manager of the Change Owner
Change Advisory Board (CAB)	A group of technical and strategic experts (membership decided by SSB) who are tasked with reviewing proposed change requests and reviewing them and approving or rejecting the changes. The CAB should either meet on a regular basis, or on an 'ad-hoc' basis to review important changes.
CAB Chair	The leader of the CAB who organizes and chairs CAB meetings and ensures that CHM processes are adhered to and meet the operational requirements of service delivery. This is normally the CHM Process Manager.
CAB Deputy Chair	The deputy of the CAB Chair who acts as the CAB Chair if the CAB Chair is unavailable.
Change Stakeholders	The stakeholders of a change are the relying parties/users/other bodies that are potentially affected or impacted by the change. These may be representatives instead of the people themselves.

Triggers

The process is triggered when a new change is determined to be high risk or otherwise would benefit from the CHM process. At this point, the RFC is created within RT in the queue corresponding to the service.

Normal change workflow

Step#	Responsible	Action	Comment
1	Change Owner	Creation of an RFC ticket in RT	Creation of a new ticket in the RT queue corresponding to the correct service. A completed RFC document is attached to the ticket, and the planned date of the change. The RFC consists of a series of standard questions asking about the type of change, testing that has been carried out and potential impact if the change is unsuccessful, in addition to rollback plans (if possible). This helps with the review of the change by the CAB.
2	Service Owner	Risk level of the change going wrong is assessed	Risk results from the Impact and Likelihood of the change going wrong. These values are defined in the RM Guideline. Calculation of risk is done by the potential impact (value of 1-4) multiplied by the likelihood (value of 1-4) of the change going wrong in the RT ticket (see RM Guidelines for more details). These values may be implemented as custom fields in RT. The risk level determines which approval authority is required to approve the change. A resulting score =<4 may be approved by the Service Owner otherwise the RFC needs to be assessed by the CAB. Any change with a risk Impact = Catastrophic needs to be assessed by the SSB.
3	CAB	Changes with risk level >4 (or candidates for standard changes - see CHM2 Maintain the list, descriptions and step-by-step workflows for well-known and recurring changes) are reviewed and approved	The CAB meets, either regularly or on an ad-hoc basis in response to an important change, to review the RFC. At the CAB meeting, the Change Owner attends to answer any questions or provide clarification about the change. If the CAB is satisfied that the RFC has been adequately prepared, approval is granted and recorded in RT.
4	Change Owner	If appropriate, the risk is signed off by informing Change Stakeholders.	Sign-off means either informing the end users and/or gaining approval from the change stakeholders. This may not always be appropriate, for example, if the change has been explicitly requested by the stakeholders.
5	Change Implementer	The change is implemented	Follow RDM2 Managing releases
6	CAB	The change is reviewed and closed	Once the change is implemented, after a suitable period of time (but not less than two weeks), the change shall undergo a post implementation review (by adding a comment to the RT ticket) and closed by the CAB. This review should be done using input provided by the Change Owner and includes assigning the quality of the change to the RT ticket (see Appendix B below), which may be implemented as custom RT fields. The implementation date of the change should be verified, and updated if it was different from the planned date. Finally the RT ticket corresponding to the change is then closed, but still searchable for future reference.

Standard change workflow

An Standard Change is a Change that is recurrent, well known change that has been submitted and approved by the CAB as a normal change (see the procedure above). Managing the list of standard changes (and further information about suitable changes that may be considered as candidates for standard changes) is described in CHM2 Maintain the list, descriptions and step-by-step workflows for well-known and recurring changes. The workflow when implementing standard changes is as follows.

Step#	Responsible	Action	Comment
1	Change Owner	Creation of an RFC ticket in RT and marks it as a Standard Change, referring it to the name of the change as listed in the wiki	Creation of a new ticket in the RT queue corresponding to the correct service, with the planned date of the change. A completed RFC document is not required for Standard Changes.
2	Service Owner	The change is considered and either approved or rejected. If it is rejected, the procedure terminates.	This can be done by discussions between the Change Owner and the Service Owner. If necessary, details of the discussion can be added to the RT ticket.
3	Change Owner	If appropriate, the risk is signed off by informing Change Stakeholders.	Sign-off means either informing the end users and/or gaining approval from the change stakeholders. This may not always be appropriate, for example, if the change has been explicitly requested by the stakeholders.
4	Change Implementer	The change is implemented	Follow RDM2 Managing releases

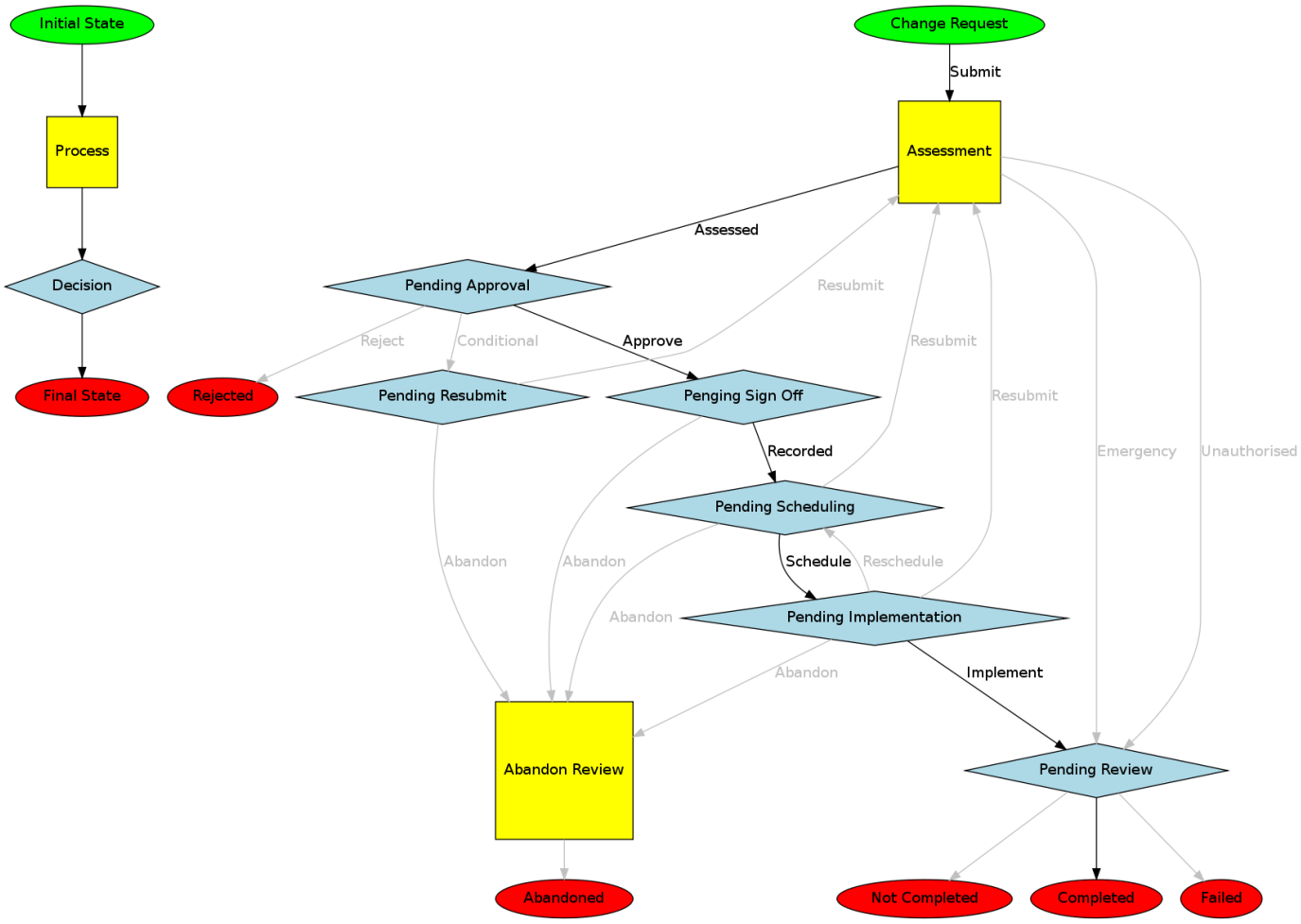
5	Service Owner	The change is reviewed and closed	Once the change is implemented, after a suitable period of time (but not less than two weeks), the change shall undergo a post implementation review (by adding a comment to the RT ticket) and closed by the Service Owner. This review should be done using input provided by the Change Owner and includes assigning the quality of the change to the RT ticket (see Appendix A below), which may be implemented as custom RT fields. The implementation date of the change should be verified, and updated if it was different from the planned date. Finally the RT ticket corresponding to the change is then closed, but still searchable for future reference. If the change was not successful, the change should be removed for the list of Standard Changes, and any subsequent change similar to it should be submitted as a Normal Change in the usual way (see procedure above).

Emergency change workflow

An Emergency Change is one that needs to be done to address a critical situation. In such circumstances it may not be practical to follow the Change Management procedure above. For example, there may not be time to get sign off from Change Stakeholders or convene the CAB to discuss and approve the change. However, it is still important for the change to be recorded. Such information will be used in a post implementation review or a serious incident review.

Step#	Responsible	Action	Comment
1	Change Implementer	The change is implemented	Follow RDM1 Managing emergency releases The change is implemented, after as much consideration of the risks and rollback scenarios as is possible given the emergency situation. Ideally this should be done by the Change Implementer consulting with another member of staff with knowledge of the service.
2	Service Owner	Creation of a change ticket in RT	A change ticket is created in RT to retrospectively capture the situation leading up to the Emergency Change, implementation of the change and outcome.
3	CAB	The change is reviewed and closed	As in Step 6 of Normal change workflow.

Workflow shown graphically



The normal workflow of a change through the process is indicated by a black line. Deviations from the normal workflow are signified by grey lines.

Schedule of Changes

All changes, both past and planned, are listed in RT. As such, it is possible to obtain a list of when past changes were carried out, as well as obtaining a list of future changes along with their planned dates.

Appendix A - Quality of change

	Description
Successful	Implementation of the change went according to the plan as described in the RFC
Problematic	Implementation of the change had some problems but these were overcome and the change was ultimately successful. Details of the problems shall be recorded in the RFC ticket.
Failed	The change did not complete successfully and had to be rolled back or worked around by following unplanned procedures. Details shall be recorded in the RFC ticket.