IT Change Management Policy & Procedure

Document Type	Policy and Procedure
Document owner	Director of IT Services
Approved by	Executive Team
Approval date	9 November 2023
Review date	31 October 2025
Version	2.0
Amendments	Revisions to all sections to provide clarification
Related Policies & Procedures	N/A

1. SCOPE

1.1 This procedure applies to IT systems and services managed or owned via London. The MRC Units in The Gambia and Uganda will have their own procedures for locally managed systems and services.

1.2 All proposed changes to IT systems or services must follow the IT Change Management Procedure.

1.3 This applies to new digital systems/services and amendment of existing ones. It includes cloud and hosted services, those developed and managed in-house by IT or other LSHTM departments.

1.4 It applies to systems and services employed to support LSHTM's institutional business operations as well as those employed as part of specific research programmes or otherwise localised within departments (i.e. managed outside ITS).

1.5 The "Go Live" of all new and upgraded services will be carried out under the Change Management Procedure. Only authorised changes to live systems are permitted and there is zero tolerance for unauthorised changes.

2. PURPOSE

2.1 A robust and mandatory change management procedure is required in order to maintain the integrity, security and availability of IT systems and services and the data they store and process.

2.2 It is the responsibility of IT Services to manage the lifecycle of all IT systems and services supporting LSHTM's business function.

2.3 The Change Management Procedure ensures a viable implementation plan is in place, adequate testing and success validation has been performed, as well as taking account of issues of data protection and cyber security.

3. Change Definition

3.1 A change is defined as anything that alters, modifies or transforms the digital operating environment or standard operating procedures of any systems or services that has the potential to affect the stability and reliability of IT infrastructure or disrupt the business of LSHTM.

3.2 Changes may be required for many reasons, including, but not limited to:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data centre, etc)
- Unforeseen events
- Periodic Maintenance

3.3 There are two routes for change permitted:

- Pre-approved (i.e. routine changes not requiring CAB approval)
- Change Advisory Board (CAB) approved

3.4 There are three categories of change:

- **Routine** – Low risk, low impact usually routine changes that are limited in scope such as those frequently carried out or repeatable in nature are pre-authorised and do not require CAB approval. This is the case where there is an accepted/ established procedure to provide a specific change requirement i.e. there is a high degree of confidence in the success of the outcome. Routine changes will have a defined trigger to initiate the change.

- **Standard** – Changes that cannot be categorised as routine (i.e. they are not low risk/minor in scope and there is no pre-established change procedure in place under which the change qualifies) will proceed through all steps of the Change Management Procedure. There are 3 types dependent on anticipated risk and impact:
  - Minor – low risk (such as a change on a software product which is used infrequently by a small group of users in one section at LSHTM e.g. CureME database system)
  - Medium – medium risk such as a change to a piece of software which is used heavily by a whole department – e.g. Registry Admin Portal)
  - Major – high risk (such as a change to one of the essential functions or an upgrade to a core piece of infrastructure which are LSHTM wide and would potentially impact the entire institution e.g.HR/Payroll *or* the MyFiles storage hosts. These are usually more significant in scope than those categorised as routine changes.

- **Emergency** – Any unscheduled change requiring immediate implementation to address an issue that is causing or likely to cause significant impact to the Business. Emergency changes are more prone to disruption and failure and thus must be managed carefully and in some unavoidable situations. Emergency changes should be notified to the Change Manager and a retrospective submission made to the CAB. Emergency changes have the same authorisation procedure as Standard Changes the only difference being that the Change Manager (or approved surrogate Change Manager i.e. Team Leader) will circulate the request via email and can authorise the Change alongside at least one other member of IT Senior Management. Emergency Changes should not be used for late or poorly planned change requests and should be only used to urgently fix or avoid a Major Incident (e.g. firmware bug on the server infrastructure has resulted in service downtime for MyFiles and is affecting all LSHTM users)

4. CHANGE MANAGEMENT PROCEDURE

4.1 Gateway

- **New Services:**
  The initial step for any potential new system is to contact the ITS Business Partners in the Information Security and IT Compliance Team. All enquiries regarding digital requirements should be directed to them first. They will guide through the subsequent governance requirements, including SDA approval and/or CISB approval, as well as CAB requirements.

  Note: all governance requirements for the project to implement a new system/service must have been met before the Change Management Procedure is undertaken – see separate Guidance on the process and definition of Operational Projects.

- **Existing Service Gateway (for updates or upgrades)**
  Either the Business Service Owner for systems owned externally to IT Services, or the Technical Service Manager for systems owned by IT Services must first engage with the Change Manager in IT Services who will guide through the required process to Go-Live.

  For hosted systems (ie cloud based services) the LSHTM Business Service owner would be expected to trigger the change management procedure, including approval at CAB, for any required changes.

  N.B. it should be noted that the formal change management procedure only applies at the Go-Live stage on systems and services which are expected to go into a live production environment. Test and dev systems do not need to engage in the process.

4.2 Determine change category

- **For non-routine changes**, submit a **Request for Change (RfC) via ServiceDesk**. (this includes changes to systems managed by 3rd parties, such as cloud bases systems). All RfCs on ServiceDesk will be set to completed once implemented by selecting the most appropriate closure status on the Change Form (from the Operator Window). This data will be used to measure the effectiveness of the Change Management Procedure.

- **Emergency Change Requests**
  Emergency changes should be notified to the Change Manager by the Change Requestor/Implementer at the earliest opportunity.

  The Change Manager should consult members of CAB to obtain approval from at least one member before issuing a decision, but it is recognised that this might not always be feasible due to time constraints in needing to apply the fix.

Communication regarding Emergency Changes should still happen, (where applicable) so that customer expectations can be managed effectively around any unexpected downtime and to avoid calls to the Helpdesk.

The Change Requester/Implementer must make a retrospective submission to the CAB. Providing an overview of the change made, its success or otherwise, communication to date, and the nature of the emergency. The Change Manager will ensure this is completed.

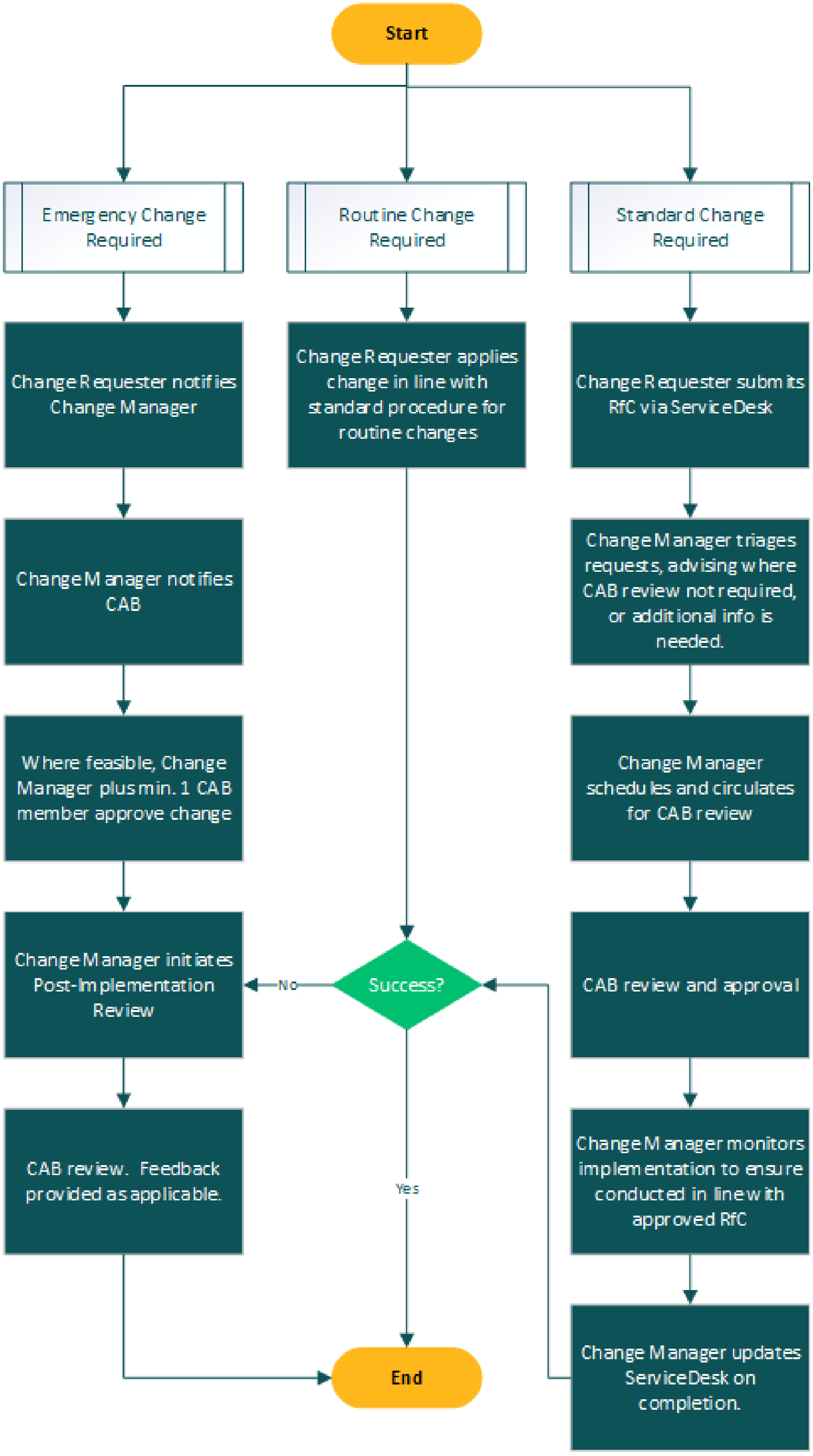
The Change Manager will investigate patterns of Emergency changes to ensure compliance with the Change Management Procedure. Escalating recurring issues to CAB and onward to the Director of ITS or the Corporate Information Services Board as required.

- **Unauthorised Changes**

  Unauthorised Changes will be logged and evaluated for continuous improvement purposes.

  Post Implementation Reviews (PIRs) will be raised by the Change Manager following identification of unauthorised changes to ensure lessons are learnt as part of continuous improvement. This will be documented and published as an Action within the RFC on ServiceDesk.

5. Flowchart - IT Change Management Procedure



Start
Emergency Change Required
Routine Change Required
Standard Change Required
Change Requester notifies Change Manager
Change Requester applies change in line with standard procedure for routine changes
Change Requester submits RfC via ServiceDesk
Change Manager notifies CAB
Change Manager triages requests, advising where CAB review not required, or additional info is needed.
Where feasible, Change Manager plus min. 1 CAB member approve change
Change Manager schedules and circulates for CAB review
Change Manager initiates Post-Implementation Review
No
Success?
CAB review and approval
CAB review. Feedback provided as applicable.
Yes
Change Manager monitors implementation to ensure conducted in line with approved RfC
End
Change Manager updates ServiceDesk on completion.

6. **APPENDIX 1**

Change Advisory Board – Terms of Reference

Parent – Corporate IT Services Board (CISB)

Purpose

- To have oversight of and make informed collective decisions on all substantial proposed changes to LSHTM IT systems and services in line with the IT Change Management Procedure to ensure an adequate change control environment.
- This involves evaluating proposed changes to ensure an appropriate roll out plan is in place, including: a properly completed RfC, which includes identification of dependencies (systems, stakeholders), consideration of risks, impact, cost effectiveness, communication to users, testing, and validation of success. The aim is to ensure delivery of a structured approach to the transition of services from the current state to desired state with minimal disruption to the customer.
- To schedule and prioritise changes by ensuring that the proposed implementation time is appropriate and does not conflict with the business need, other change or operational activities.
- Make recommendations to reduce risk, increase likely success, and minimise business impact, ensure value for money, and build awareness of upcoming changes in the user community.
- To reduce disruption and outages caused by unauthorised, failed or poorly considered and managed changes. Improving customer experience.
- Ensure that business outcomes are documented and well understood and that the proposed Change will give the intended outcomes without adversely impacting the business.
- To embed and drive understanding of and compliance with the Change Management Procedure across LSHTM.
- To ensure issues of information governance and cyber security have been duly considered where these are a factor in any change request.
- To enable quick and accurate changes based on business priorities.
- Highest priority should be given to ensuring LSHTM's systems and services comply with relevant legislation and have adequate steps in place for protection of information assets, systems and services from attack.
- To identify and address any on-going issues, escalating as appropriate to the CISB.
- To monitor Key Performance Indicators to evaluate the success of LSHTM's Change Management Procedure and control environment. Use these to inform any future amendments to the procedure which will be authorised by CISB.
    - Number of changes implemented in the reporting period broken down of changes by system/service
    - Increase in the number of successful Changes
    - Reduction in the number of failed, backed out or cancelled Changes

- Reduction in the number of Major Incidents (outages) resulting from Changes
- Reduction in the number of incidents resulting from Changes
- Reduction in the number of unauthorised Changes
- Reduction in the number of unplanned Changes/ emergency Changes
- Number of Changes rejected by the CAB

Membership / Roles & Responsibilities

The Change Management Procedure is dependent on a number of roles being performed and responsibilities being fulfilled as set out below.

Role	**Responsibility**
Change Manager	Responsible for the management of RfCs. Chairs the CAB meetings
Change Requestor	Responsible for raising/ submitting the RFC, building and implementing the authorised change.
Technical Service Manager	The ITS member of staff responsible for the delivery of the service to the Business and approving the RFC.
ITS Heads of Service	Infrastructure & Architecture, Information Security & Compliance, Enterprise Systems & Web Services, Operations and Support
Business Service Owner	Outside ITS, the person or a delegated representative, with ultimate accountability for the provision of a Service to the organisation and approving the RFC.
Project Manager	Responsible for the management of projects and the raising of project related RFCs for submission to the appropriate CAB.
ITS Services Manager	Responsible for advising and guiding the Change Requestor on the most appropriate communications strategy to be used for communicating the proposed changes and its impact.
IT Business Partner	Point of contact for advising Faculties and Professional Services departments of proposed changes affecting their areas.

Project managers or business service owners may be invited to CAB to answer queries on the proposed change.

Meetings

- Change Advisory Board will meet every Wednesday at 2pm to review Requests for Change.
- If attendance by a CAB member is not possible, they should either review and feedback comments before the CAB or nominate an appropriate delegate to represent them.
- If the Change Requestor is not present at CAB then the change will not be discussed and cannot be approved
- RfCs may be approved by email outside the meeting where proposed by the Change Manager and agreed by all CAB members.

7. APPENDIX 2

Examples when a Request for Change submission to CAB is and is not required:

Routine Change – No RFC

- Replace single server in a cluster – there is a recognised process for this and no user impact is expected, therefore no RFC is required.
- Replace a single network switch - this has user downtimes so the first time this is required it would be submitted as a **standard medium change with an RfC** - once the process has been seen to be successful this would be **switched to a routine change and no further RfC is necessary**
- Regular security patches that have been fully tested in the dev environment

N.B.

- A POC and pilot are generally considered outside of change control when they involve user testing as they will bring to the surface many factors that may not have previously been considered.

Standard Change
Minor

- Upgrade to Graphpad Prism – small number of users and is not a regular occurrence. Is user affecting
- Go-live of individual database for a specific team – all new systems that go-live must have an RfC, but this is a small service for a small group of users

Medium

- Upgrade to MyFiles services – used across the institution, not a regular occurrence but is no longer used by all staff/students, so would be a
- Go-live of a new service for a whole department – all new systems that go-live must have an RFC and this is used by more than a few users

Major

- Point release of a business system upgrade (e.g. Agresso 5.x to 6.x) = review release notes, talk with Change Manager submit Standard RFC.
- Point release of an existing hosted service, eg Moodle - although this is not an LSHTM managed service it is under contract, and should therefore be under supplier management so would still need to go through the normal RfC process. It is also a heavily used service across the whole student body.
- Go-lice of a new essential function service, eg HR/Payroll – institution wide service with huge impact. As with all go-live situations a full RfC is required

Emergency Change

- Release a fix to a live service that has directly impacted a large number of users (e.g. core router has suffered a bug which has prevented all external access - **Emergency Change where the RFC can be submitted retrospectively**
- Core piece of infrastructure has been identified by the supplier as containing an exploitable vulnerability which they have released an emergency fix for (e.g. heartbleed) – this has the potential to massively negatively affect LSHTM and as such needs to be secured rapidly – **emergency change with eCAB approval and retrospective RfC**