Standard Operating Procedures (SOP) for:			
Configuration Management and Change Control			
SOP Number:	**DG25**	Version Number:	**1**
Effective Date:	**14/07/2014**	Review Date:	**14/07/2015**

Author:	**William Mordaunt, IT Services Project Manager**
Reviewer:	**John Steel, Assistant Director Customer Services 19/05/2010**

Authorisation:	
Name / Position	**Chris Day, Acting Director of IT Services**
Signature	**C Day**
Date	**26 October 2010**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Change Requestors Configuration Manager Change Manager Change Assessors Change Implementers

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	12/05/2010
1	Annual Review – No change	Alan Hardy	14/07/2014

Purpose and Objective:

To ensure that configuration management and change control are performed in accordance with industry best practice.

To define standards for configuration management and change control. The change control process includes both planned changes and emergency changes. Planned changes are those which are planned in advance, e.g. upgrades, additions, or decommissioning of infrastructure or systems. Emergency changes are those which are required to respond quickly to unforeseen events, e.g. infrastructure failures, system failures or security breaches.

The change management process described in this procedure applies to the production environment and not development or test environments. The process is intended for infrastructure related changes which may potentially affect multiple users.

This process covers services which are managed by IT Services.

What is a Change?

A change is any alteration to a service or service component that may have an impact on the quality of service delivered to the customers of that service. As such all service changes will need to be appropriately managed and controlled.

Why do we need Change Management?

1. The Director of IT Services is accountable for the availability, operability and maintainability of services delivered to QMUL. The Customer Services Group within ITS has been delegated responsibility for acting as gatekeepers for ensuing that IT changes do not jeopardise any of the services that are delivered.

2. A holistic view of IT change across the whole of QMUL provides greater understanding of the potential impacts and resource demands.

3. Better management of risk and financials by exploiting opportunities to package IT changes into releases. This also includes performing a business/technical impact assessment of small enhancement type requests.

4. Higher service availability via independent assurance of the quality of change products that are delivered.

5. Change implementation planned and scheduled in context with all other IT change activity; mitigates risk of potential change conflicts.

6. Ensures all aspects of IT change have received due consideration, including business impact analysis where appropriate, before they are implemented.

7. Facilitate brokering of IT change with the Faculties to resolve prioritisation of IT changes that can impact their business operations.

8. Better monitoring and reporting of IT change which will facilitate service improvements that provide a better and more responsive IT change service to QMUL.

9. Facilitate operational efficiencies by identifying and sponsoring proposed changes for consideration as standard changes e.g. service requests.

10. Ensure that return to normal operations is performed in a controlled manner with the retrospective review and approval of changes performed as part of any emergency.

SOP Text

Configuration Management

	Responsibility	Activity
1.	Director of IT Services	A register shall be established and maintained in LANDesk providing a repository of configuration data for information processing systems. This shall include, for example, details of servers and network devices.
2.	Configuration Manager	Configuration data for information processing systems shall be recorded and maintained in the configuration repository.

3.	Configuration Manager	Configuration data shall be updated after changes have been made to information processing systems.

Change Control – Planned Changes

4.	Director of IT Services	A change register shall be maintained in LANDesk providing a record of all requests for change (RFC) to production systems within the scope of this procedure. Refer to Appendix A Change Control Scope for guidance on the scope of changes governed by this procedure.
5.	Change Requestor	A formal RFC shall be raised and submitted to the Change Manager to log in the change register describing the proposed change to a production system. Refer to Appendix B for example of contents of the RFC form.
6.	Change Manager	Receives, logs and allocates an initial category and priority with reference to existing RFCs and in collaboration with the Change Requestor. Initiates emergency Change Procedures if RFC is deemed to be an emergency change. Any impractical RFCs are rejected at this stage. Refer to Appendix C for definition of Change Categories.
7.	Change Manager	Identifies Change Assessors based on service assets and configurations affected and issues appropriate RFCs for impact assessment.
8.	Change Assessors	Perform impact and resource assessment for the RFCs referred to them using a risk-based assessment. The Change Assessors need to consider: • Impact the change will have on the Customer's business operations • Effect on the infrastructure and service • Impact on other services that run on the same infrastructure • Impact of not implementing the change • Resource considerations • Impact on non-IT infrastructure e.g. helpdesk • Current Change Schedule and Projected Service Outages • Impact on other Service Management areas including continuity plans
9.	Change Manager	The configuration data/documentation that will need to be updated as a result of the proposed change shall be identified and recorded in the change register.

10.	Change Manager	Collates assessment feedback and updates change register.
11.	Change Manager	Tables new RFCs for a change advisory board (CAB) meeting, issues the agenda and circulates the RFCs to CAB members in advance of the meeting. Formal approval for the proposed change shall be sought. Proposed changes shall be reviewed by a change advisory board. The composition of the CAB shall be based on the RFCs under consideration but its core member shall be the: • Infrastructure Services Manager • Application Services Manager and • Service Delivery Manager
12.	Change Manager	After consideration of the advice given by the CAB members, authorises acceptable changes.
13.	Change Manager /Requestor/ Implementer	A date and time for making the approved change shall be scheduled. This shall be during an agreed regular maintenance window where possible to minimise disruption to normal business operations.
14.	Change Manager	Publishes CAB minutes, updates projected service outage and issues change schedules via ITS Helpdesk.
15.	Change Manager	Details of the approved changes shall be communicated to all relevant people/organisations.
16.	Change Manager	Updates the change register with all progress that occurs.
17.	Implementer	The change made shall be built and tested using the process described and recorded in the change register.
18.	Implementer	The approved change shall be made to the production system.
19.	Implementer	If the change was unsuccessful then it shall be reversed using the procedure defined in the change register.
20.	Change Manager	On successful completion of a change (or the rollback of an unsuccessful change) the outcome shall be communicated to all relevant people/organisations following the communications plan recorded in the change register.
21.	Configuration Manager	The configuration data/documentation identified and recorded in the change register shall be updated as a result of the change.

22.	Change Manager	The RFC in the change LANDesk shall be updated to show the change item is closed.
23.	Change Manager	Conducts Post Implementation Review, particularly for failed changes and high impact changes so that lessons can be learnt and incorporated into the change process.
24.	Change Manager	Closes RFCS and produces regular and accurate management reports.

Change Control – Emergency Changes

25.	Change Requestor	Formal approval for the proposed change shall be sought. Emergency changes may be authorised by the Director of IT or their deputy and a retrospective RFC raised for formal review and evaluation.
26.	Change Manager	Receives and logs the emergency change RFC.
27.	Change Manager	Identifies impact assessors based on service assets and configurations affected and issues appropriate RFCs for impact assessment.
28.	Change Assessors	Perform impact and resource assessment for the RFCs referred to them using a risk based assessment. The Change Assessors need to consider: • Impact the change will have on the Customer's business operations • Effect on the infrastructure and service • Impact on other services that run on the same infrastructure • Impact of not implementing the change • Resource considerations • Impact on non-IT infrastructure e.g. helpdesk • Current Change Schedule and Projected Service Outages • Impact on other Service Management areas including continuity plans
29.	Change Manager	Consolidates assessment feedback and updates RFC register.
30.	Change Manager	Issues RFCs to the Emergency change advisory board (ECAB). Formal approval for the proposed change shall be sought. The composition of the ECAB shall be based on the RFCs under consideration but its core member shall be the: • Infrastructure Services Manager • Application Services Manager and

		• Service Delivery Manager
31.	Implementer	The change shall be tested.
32.	Implementer	The approved and tested change shall be made to the production system.
33.	Implementer	If the change was unsuccessful then it shall be reversed using the procedure defined earlier.
34.	Change Manager	On successful completion of a change (or the rollback of an unsuccessful change) the outcome shall be communicated to all relevant people/organisations.
35.	Change Requestor	A retrospective formal RFC shall be raised and submitted to the Change Manager.
36.	Configuration Manager	The configuration data/documentation identified and recorded in the change register shall be updated as a result of the change.
37.	Change Manager	Conducts Post Implementation Review, particularly for failed changes and high impact changes so that lessons can be learnt and incorporated into the change process.
38.	Change Manager	Closes RFCS and produces regular and accurate management reports.

List of appendices

Appendix	**Appendix name**	**Location**
Appendix A	Change Type	On page 7
Appendix B	Contents of RFC	On page 8
Appendix C	Change management Scope	On page 9
Appendix D	Change Categories	On page 10
Appendix E	Change Advisory Board	On page 10

What is a Change?

A change is the addition, modification or removal of anything that could have an effect on a production IT service

Appendix A - Change Types

The table below gives examples of changes described in this procedure. It is worth noting that **ALL** changes are subject to the change Management process.

Standard Changes	Non-standard Changes (Normal Changes)	Emergency Changes
A Standard Change is a pre-approved, relatively common, well known, documented, low risk Change. The change activity normally happens frequently and would not normally require any scheduling or communication beyond informing a user or small group. As such, it is quite common for a Standard Change (SC) to have previously been a Non-Standard Change (NSC) which has been approved by the appropriate Change Authority to become an SC and CAB notified. Standard Changes will be often implemented after being requested via the Request Fulfilment Process some of which might have been directly recorded and passed for action by the Service Desk.	A Non-Standard Change (Normal Change) is a change that is neither an Emergency Change nor a Standard Change. Normal changes follow the defined steps of the change management process. Simply put, an NSC is actually defined by what it is not. Since it is not a standard change nor an emergency change, it is simply every other change and must be authorised. An NSC requires additional information to Standard Changes.	The Emergency change procedure is reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Emergency changes should be designed carefully and, if possible, tested before use or the impact of the emergency change may be greater than the original incident. Emergency changes may document some details retrospectively. The number of emergency changes proposed should be kept to an absolute minimum, because they are generally more disruptive and prone to failure. All changes likely to be required should, in general, be foreseen and planned, bearing in mind the availability of resources to build and test the change. Nevertheless, occasions will occur when emergency changes are essential and so procedures should be devised to deal with them quickly, without sacrificing normal management controls.

Appendix B – Contents of a RFC

- Unique Number
- Change Trigger
- Description of Change
- List of Configuration Items to be Changes
- Business Case for Change
- Change Priority
- Effect of not Implementing the Change
- Change Requestor Contact Details
- Change Category - Minor, Significant, Major
- Predicted Timeframe/Resource/Cost
- Initial Risk and Impact Assessment
- Test Plan
- Communications Plan
- Back Out Plan
- Configuration Data and Documentation to be updated
- Impact on Service Continuity, Capacity, Security, Test Plans

Appendix C -Change Management Scope

Based on our chosen context for our Change Management process the following are examples of changes in scope for Production environment:

Hardware	Systems Software	Applications Software	Artefacts
Adding to capacity	Operating system changes such as new releases or patches	Using an administrator account to modify a setting that changes the behaviour of an application	an IT policy
Replacing hardware that is being taken out of service (e.g. lifecycle)	Security software changes	Using the email application as an example, changes might include revised quotas or the handling of spam emails	an IT process
Installing new hardware to support a new or existing service	Anti-virus software or virus definition update	A new release of an application that provides business functionality	an IT standard
Substituting an identical piece of equipment and configuration, even if the Configuration Item (CI) attributes has not changed.			an IT SOP
A break-fix replacement of a faulty router of identical type and configuration			an SLA or OLA
Removing/retiring end-of-life hardware			High Level Design / Low Level Design / Schematic Diagram

Appendix D - Change Categories

Size	Description
Major	Large impact changes, and/or will require large amount of resource to implement, and/or impact more than one Faculty. Changes to multiple related Configuration items are likely to be managed as a release.
Significant	Changes that may be more complex and/or have large implementation resource requirements. Such changes will more thorough impact assessment than a minor changes.
Minor	Small / operational changes that are relatively low risk requiring minimal impact assessment. **Note** CAB will be informed of minor changes but will not be expected to review them.

Appendix E - Change Advisory Board

Purpose

- To support the change approval process by assessing the impact of proposed changes and supporting (or not) the implementation of change.
- Assist the Change Manager in the prioritisation and scheduling of change implementation.

Objectives

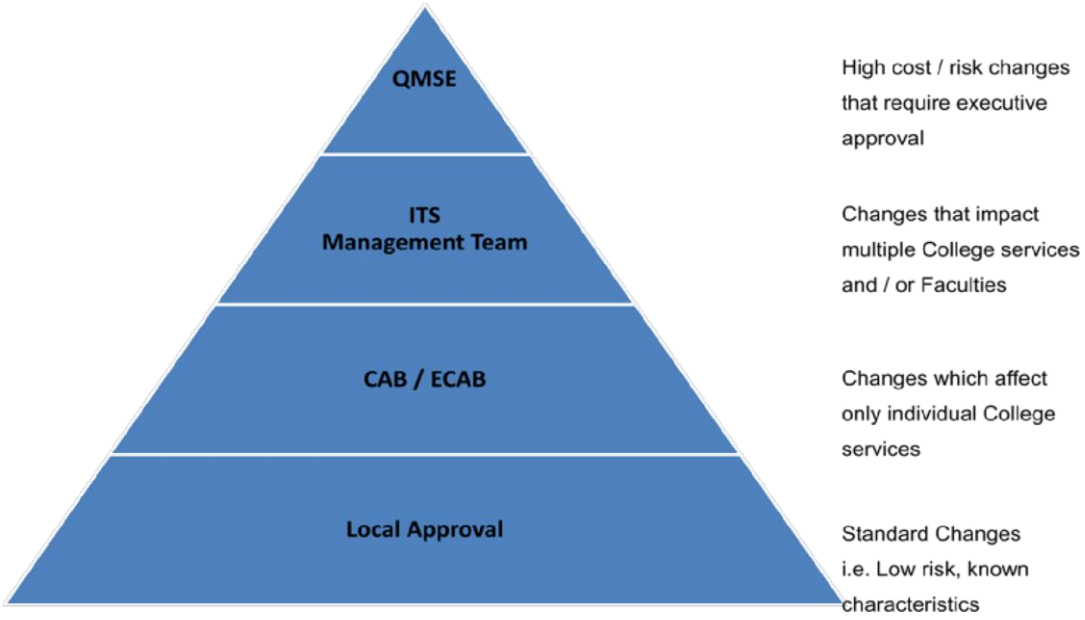
- To recommend the approval to implement IT changes to College services on behalf of the Director of IT Services.
- To act as change quality gatekeepers to ensure that changes are backed up by required change deliverables.
- To ensure that risks and costs of making changes to live services are fully understood and documented.

Goals

- To ensure that all live IT service changes to any production College service have been reviewed and approved by the appropriate level of Change Authority.
- To ensure that all live service change requests are supported by the minimum set of change deliverables.

- To ensure that the CAB members receive all of the information necessary to enable an objective assessment of the change.

Change Governance Structure



CAB Supporting Mechanisms

- Recipients notified of CAB meeting via email with attachments
- CAB meeting minutes published within 1 business day of meeting
- Projected service outage and change schedule updated and published within 1 business day of meeting

Interfaces

Inputs	Outputs
Operational Changes – Defect Fixes – Small Enhancements	• **CAB minutes** • **Change Schedule/Calendar**
Tactical Changes – Project Enhancements	• **Projected Service Outage** • **Change Approval Notifications**

Strategic Changes – Major Releases	

CAB Agenda

- Review changes larger than Min or changes that have been assessed by the CAB members

- Agree revised change schedule and projected service outages
- Review any major change implementations e.g. New Releases
- Review the advance notification of changes that are to be presented at the next CAB meeting (pipeline).
- Periodic review of the performance (effectiveness and efficiency) of the QMUL change process