UCD IT Services Change Control Process (February 2024)

Introduction

This document describes the overall Change Control Process used in UCD IT Services, and how central and local change control processes work within the Unit.

1. What is Change Control

A change is the addition, modification, or removal of anything (systems, services, functions, features, controls, processes, procedures) that could have an impact on IT systems / solutions.

The purpose of the change control process is to enable beneficial changes to be made in a planned and controlled manner with minimum disruption.

Changes include both those delivered as formal projects driven through the Work Programme, operational changes undertaken as service delivery/continuous improvements projects, and regular support tasks/activities.

All changes delivered as IT projects must follow the requirements outlined in the PMO framework.

Change Control is used in the Planning and Executing Phases of the project lifecycle (including those spun out from support activities – such tasks have equivalent planning and executing steps).

Proposal	Initiation and Discovery Phase	Planning Phase	Executing Phase	Close-Out Phase
		Design Approval & Enabling Works	Go-Live Approval	

Mapping Change Control to the PMO framework

2. Changes Type

There are four types of change.

Type 1 / LOCAL
Straightforward, Routine, Frequent
Authorised by local CAB

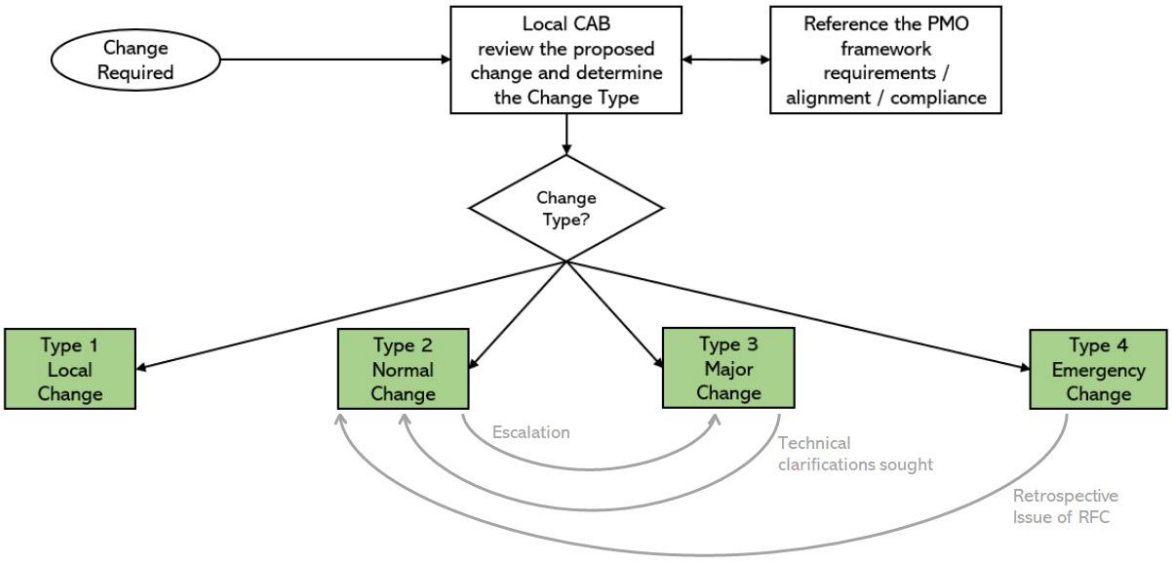
Type 2 / NORMAL
Important
Full review
Authorisation by CCB required

Type 3 / MAJOR
High Risk
Full review
Authorisation by ITLG

Type 4 / EMERGENCY
Urgent
Resolves incident
Flexible pool of approvers

All changes should go through the local change review process before any "normal" or "major" change is submitted to the CCB. This ensures that all relevant expertise is considered and that the person presenting the change can adequately represent the change at the CCB meeting.

The change type determines the ultimate change authority required, and the acceptance/ approval process that must be followed.



3. Change Priorities

There are two priorities of change.

Priority 2 / NORMAL
Non-time critical change.

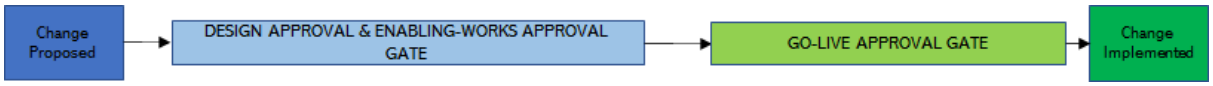
Priority 1 / HIGH
Time critical change or change requiring reallocation of resources.

Change will be reviewed at the next regular change control meeting	Emergency change control meeting to be called

Change requests will be reviewed by the CCB based on priority, with changes identified as Priority 1 being assessed ahead of Priority 2 changes.

4. Change Control Gates

There are two key "change approval gates - "design & enabling-works" and 'go-live'.



The design & enabling works approval gate is an assessment and review and occurs in the Planning Phase of a project.

The change owner presents a high-level overview of the proposed change, how technical, security, architecture and support requirements will be met, and any preparatory/enabling works (such as network changes or integrations) that need to be made.

This will allow the CCB to assess the design, and authorise the technical deployment/implementation (but not go-live).

The go-live approval gate is in the Executing Phase and is a mandatory final sign off required before the change is transitioned into production. It ensures that change requests have been documented and recorded and signed off as meeting technical, security, architecture, support, and communication requirements.

5. Change Control Board

The Change Control Board is the central technical design authority regarding all changes within the IT Services department.

The Change Control Board acts as a "change gate", allowing proposed changes to move through the Project Phases from Planning, through Executing, to Closing.

Change Control Board (CCB) membership comprises the following, representing disciplines across IT Services, allowing informed assessment and compliance of proposed changes.

Area/Discipline	Member(s)
Communications	Sinead O'Rourke
Customer and Academic Services	Eoin Hanratty, Caroline Hackman
Infrastructure	Anthony Grenham, Eoin Wickham
Enterprise Applications Group	Peter McKiernan
IT Security	Paul Kennedy
Enterprise Architecture	Tom Cannon (Deputy Chair)
IT Leadership Group	David Coughlan (Chair)

Where a member is not available for a CCB meeting, they are asked to nominate someone to attend in their place.

6. Change Control Meeting

The Change Control Board will meet monthly (the first Wednesday of each month) to review and approve proposed changes based on an assessment of technical solution, security, risks, architectural alignment, and support. In the case of an emergency change, a retrospective review may be required.

Items for assessment by CCB need to be submitted at least a week in advance.

The CCB may call to the Change Control Meeting anyone that it is felt needed to adequately inform the assessment and compliance of proposed changes.

The Chair of the CCB will report any key decisions to the IT Leadership Group on a monthly basis.

RFCs must be submitted by the last Wednesday of each month, for review by the CCB the first Wednesday, with a decision issued by the CCB the following day.

This is based on the expectation that when change requests are submitted, the change owner has already confirmed with all necessary stakeholders, including the CCB that all requirements have been met and alignments adhered too.

It is recommended that relevant members of the CCB are involved in the development of the Change Requests ahead of submission to address potential issues, particularly around technical, security, architecture, support and communication requirements and alignments.

If the above has not been undertaken, or the RFC and support documentation are incomplete or unclear, the approval process will take longer.

7. Local Change Advisory Boards

Quality and Change Advisory Boards (QCAB) are the local change authority regarding local changes, within teams and verticals. They assist the CCB in assessing the type and priority of changes and ensuring that the relevant information relating to the changes are passed to the CCB as required.

8. ITLG Escalation

Where the CCB identifies a risk or concern that requires escalation to the ITLG, this is done by the CCB chair (or nominee) sending details of the risk or concern, along with summary of the advice and/or clarification(s) sought.

9. Weekly Operations Meeting

The weekly IT Operations Meeting is a separate forum used for tracking and communicating the Forward Schedule of Changes – which lists all approved changes along with their scheduled implementation dates.

On occasion, and as deemed desirable, the CCB may require that the change owner presents a proposed and/or approved change at the weekly Operations Meeting

10. Data Protection Impact Assessment

For all changes, the change owner must consider data privacy and data protection for GDPR purposes. Where personal data is involved or at risk, at the planning stage a set of Screening Questions must be completed to determine if a Data Protection Impact Assessment (DPIA) is required.

Where required, copies of the completed Screening Questions Template and IT Services DPIA Template should be sent to the Data Protection Officer (DPO) at gdpr@ucd.ie. Where high risks to personal data have been identified, advice should be sought from the DPO before proceeding with the change and any mitigating actions incorporated into the scope of deliverables.

The CCB will not be reviewing the Screening Questions or DPIAs but as part of the CCB go-live approval process the CCB will ask if they have been completed and the CCB must be advised if there are any aspects the DPO raised that have not been fully addressed.

11. IT Security Review

For all changes, the change owner must consider if a Security Review is required. As a general guide, a security review should be undertaken on new implementations of IT systems or solutions, on premise or in the cloud, that process personal data or confidential university information, or when existing solutions are being upgraded. See the IT Security Review Process document for further details.

12. Testing and Quality Assurance

All changes must be robustly tested and signed off by both the Business and IT owners. This includes;

- Unit/Component – test individual components of the system.
- System Integration - test all interaction between systems that the changed system integrates with.
- Functional - in abstract, does application work as expected.
- User Acceptance - in context, does it meet business requirements.
- Load/Volume/Performance/Stress/Scalability - does it work under expected real-world workloads.
- Disaster Recovery testing – restoration of the service and data after a simulated IT failure, within the required recovery time and point objectives.

13. Proof-of-Concepts and Pilots

It is expected that Pilots - implementations to evaluate how a solution performs under real conditions / typically a small number of schools or units - follow the change control process and should be assessed by the CCB. Simple PoC projects - implementations to test the feasibility of a solution, limited to a small group of users – are assessed by local QCAB.

14. How to Submit a Change (Detailed Overview of Change Types & Change Procedure)

The following tables provides an overview, and examples, of each change type to assist in this self-assessment, and the processes that then must be followed.

Where there are concerns around any planned change, or an assessment by an IT stakeholder or local CAB judges that the proposed change is a Type 2 (e.g., potential for significant impact on support services, a significant security concern) then the change must be treated as a Type 2 change.

After approval only minor changes deviations from the change request may be applied without invalidating the original approval and requiring the change to the resubmitted to the CCB for assessment.

Deviations during 'go-live' implementation must be included in the Post Implementation Review.

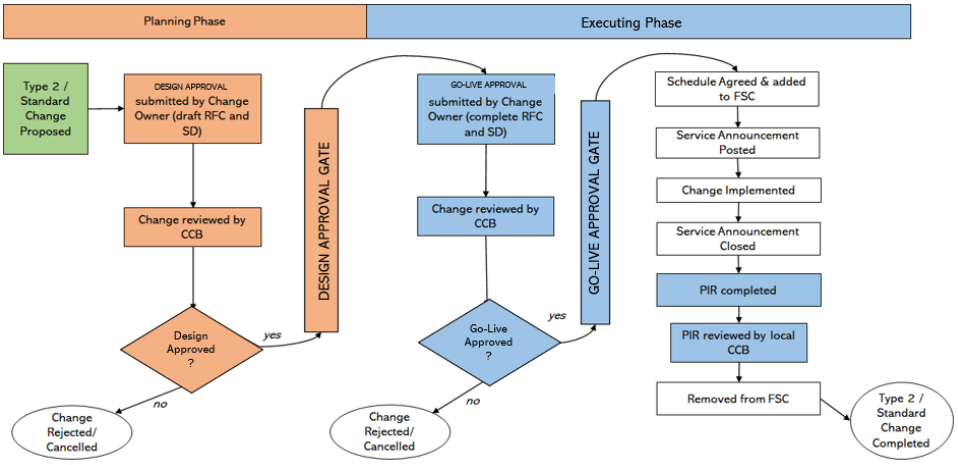
Change Type - 1 / Local

Description	Frequent, routine, straightforward changes that follow well-established procedures.
Examples	• Routine Updates • OS/Application Patching • Creation, or changes to reports, reporting information, database tables/structures. • SSO integration of systems/applications outside of the IT System Portfolio using standard attributes. • Pre-approved changes (These are changes that have been previously assessed by the CCB and it has been determined that subsequent changes following the same process are also approved, and don't need to be referred back to the CCB for subsequent evaluation. This is often applied to upgrades to SaaS solutions once the CCB is cognisant of the upgrade/update process, and has approved the method) • Business as Usual changes • User Interface changes where the support impact is minor, and both well understood and accepted by Customer Services • Opening/Closing Network Access where there is no perceived significant security or support impact (ACL and/or firewall rule changes to non-critical / sensitive networks) • Changes to Test and/or Development systems (including Business Systems, Network Load Balancer, Server Farm and Research) where there is no production or sensitive data involved.

	• Any network access changes related to 80 and 443 on the general wired and Wi-Fi networks • Proof of Concepts (PoC) – implementations to test the feasibility of a solution, limited to a small group of users (typically the project's core team itself).
Change Control Authority	Local
Handling of Change	Change DESIGN APPROVAL and GO-LIVE APPROVAL is done by local CAB/manager/team. The implementation of the pre-approved change is brought to the weekly IT Ops meeting for inclusion in the Forward Schedule of Change (FSC) by the Change Owner.
Further Notes	Where there is an impact on the system or service a Service Announcement must be completed (and closed on completion) Where possible local changes should be applied during the maintenance windows (for the limited cases where this is not possible, the release schedule should be agreed with the business owner). For simple changes, the design and go-live approval may be a single step/action.

Change Type - 2 / Normal

Description	Important and/or non-trivial changes made to IT systems, services, or infrastructure.
Examples	• Major Application Upgrades. • Adding Functionality or significant changes to the User Interface. • Significant changes to systems, services, functionality, service or security architecture, or the dependency on, or integration provided to other systems/services. • Changing the authentication method and/or SSO integration of systems/applications in the IT System Portfolio. • SSO integration of systems/applications outside of the IT Services portfolio, using non-standard attributes (aka release of specific user attributes). • Change that could reasonably be expected to impact users, impact support, or require additional calls to the IT Helpdesk. • Changes with unknown, unqualified, or unquantified customer impact. • Addition or removal of systems from the IT System Portfolio • Where the DPIA identifies that there is a medium or high potential of risk to the rights and freedoms of data subjects

	• Any network access changes to the Business Systems Network, Network Load Balancer, Server Farm Network and Research Network involving production systems, or where production or sensitive data is involved • Any network access changes other than 80 and 443 on the general wired and Wi-Fi networks • Any network access change where there is a perceived significant security or support impact • Pilots – implementations to evaluate how a solution performs under real conditions / typically a small number of schools or units. It is expected that pilots come to the CCB for both "design/enabling works" and 'go-live" approval, noting that the 'go-live' approval covers the pilot.
Change Control Authority	CCB
Handling of Change	 Change DESIGN APPROVAL Request must be submitted during the Planning phase of a project. • Submit Request for Change, sections A (general) and B (design and enabling works), and draft System Descriptor, and any other supporting documentation (e.g. DPIA and Security reviews) that are felt useful for the CCB to make an informed assessment of the proposed change, by emailing change.control@ucd.ie • Questions may be raised and clarifications sought ahead of the CCB meeting, via change.control@ucd.ie mailing list, and should be answered back through the same channel. • Change Owner will typically be required to present the change at the CCB meeting. • The Change Owner may be required to further clarify aspects of the Change Request, before CCB can reach this decision. The CCB will then make a decision. Change GO-LIVE APPROVAL Request must be submitted during the Executing phase and approved ahead of go-live.

	• Submit Request for Change, sections A, B, and C (go-live) and completed System Descriptor,by emailing change.control@ucd.ie • Questions may be raised and clarifications sought ahead of the CCB meeting, via change.control@ucd.ie mailing list, and should be answered back through the same channel. • Change Owner will typically be required to present the change at the CCB meeting. • The Change Owner may be required to further clarify aspects of the Change Request, before CCB can reach this decision. The CCB will then make a decision. • Following approval, the Change Owner must separately ensure that the scheduled work is brought to the weekly IT Ops meeting for inclusion in the Forward Schedule of Change (FSC). • Change Post Implementation Review (PIR) must be completed within 3 days of change being completed (or attempted). This is done by updating your response to your original Google Form submission.
Further Notes	Where the CCB requires clarification from the ITLG, this should be done by the CCB chair (or nominee) sending summary details of the change and the advice or clarification(s) sought. Where there is an impact on the system/service a Service Announcement must be completed (and closed on completion) Where possible normal changes should be applied during the maintenance window (for the limited cases where this is not possible, the release schedule should be agreed with the business owner). For simple and quick changes, the design and go-live approval may be a single step/action. However it is expected that as Type 2 changes are complex, they would require separate submissions as the level of detail available at Design Sign-off will often be insufficient for Go-live sign off. When changes are submitted to the CCB, questions may be raised before the meeting via the email group, and should be answered where possible back through the same email chain so that all members of the CCB are aware of the clarifications sought, and responses.

Change Type - 3 / Major

Description	Changes with a high risk, significant financial investment, or alteration of business operations. CCB may be required to review/appraise these before they are submitted to ITLG.
Examples	Change in major underlying technologies or platforms, removal or expansions of major functionality that other systems/services are reliant on. Introduction of new policies

Change Control Authority	ITLG
Handling of Change	ITLG proposals generally outline the high level / business case for a change and are reviewed by the ITLG Team. The ITLG may direct that the change request is reviewed by the CCB. If so, follow the procedure for Change Type - 2 / Normal.
Further Notes	It is good practice to involve applicable members of the CCB in the development of the ITLG proposal to address potential issues, particularly around technical alignment, security compliance, etc... ahead of submission.

Change Type - 4 / Emergency

Description	Urgent changes, typically performed to prevent/avoid or resolve serious incidents (system/service disruption, degradation, or to eliminate a potential security risk). These changes carry significant risk and require accelerated authorisation and planning.
Examples	Emergency Changes are performed to avoid or resolve serious system/service disruption, degradation in system/service quality or to eliminate a potential security risk. Therefore, it is always related to one or more major incidents.
Change Control Authority	Flexible (ITLG member, Head of Service, or CCB)
Handling of Change	Emergency Changes are undertaken before formal RFC has been submitted to the CCB for assessment. A completed RFC must be retrospectively issued within 3 days of the emergency change being undertaken, following the procedure for Change Type - 2 / Normal.
Further Notes	It is expected that there would only be 1 - 3 emergency changes requests per year. The complexity and impact of the specific major incident and identified recovery will determine the time required to approve. The CCB may direct that follow-up changes are undertaken to ensure alignment with technical, security, architecture, and support requirements. Additionally, Incident Management, Crisis Communication and Root Cause Analysis (RCA) processes must all be followed for major incidents.

15.Appendix

Link to Request for Change (RFC) Template

Link to System Descriptor (SD) Template

Link to Data Protection Impact Assessment (DPIA) for IT Projects

Link to DPIA Screening Questions Template

Link to IT Policies and Guidelines

Link to Type 1 & 2 Change Examples

16.Glossary

CCB	Change Control Board IT Services central technical design authority, for Normal changes
Change Calendar	Change Calendar A change calendar will be maintained by the CCB showing frozen zones, blocked maintenance windows and changes with their criticality listed. The change calendar should forecast the year ahead to allow for planning.
FSC	Forward Change Schedule This is maintained by the Ops chair. It tracks all scheduled work taking place.
local CAB / QCAB	Local Change Advisory Board / local Quality and Change Advisory Board Local change control authority, for local changes.
PIR	Post Implementation Review Completed after all changes to advise the CCB whether there was any deviation from the agreed plan.
RFC	Request for Change The Request for Change is used to identify, quantify, and capture the planned change – to explain the change, breakdown the complexity, identify and counter the risks, identify all the resources required and how customers/users will be impacted.
SD	System Descriptor System Descriptor describes the overall architecture of each system, broken down into the constituent part of how the system is designed, delivered and supported.

17.Version History

Name	Version	Date	Reason for change
Tom Cannon	6.0	11/5/18	-
Tom Cannon	6.99B	1/12/20	Updated following initial ITLG review. Reduced CCB, change from minor to local terminology, and provided clear demarcation between CCB and Op processes.
Tom Cannon	6.99C	8/12/20	Update following ITLG review. Change of meeting frequency from weekly to monthly.

Tom Cannon	7.00	17/01/22	Update approved by the ITLG. Update includes; • additional changes, examples and inclusion of a "treat as a type 2 if in doubt" note. • updates to DPIA section, including revised requirements, and links to Screening Questions • additional clarity in definition of sensitive network changes, and that all changes must follow the requirements outlined in the PMO framework. • ITLG Escalation
Tom Cannon	7.10	28/11/22	Update to include reference to procurement and non-functional requirements
Tom Cannon	7.11	10/01/23	Add the Testing and Quality Assurance section, at request of external auditors.
Tom Cannon	7.12	18/01/23	Removal of procurement section.
Tom Cannon	7.13	13/03/23	Rework of the approval stage gates, to add 'design approval' at the initiation phase.
Tom Cannon	7.15	27/03/23	Reworked back into 2 phases – "design and enabling" and "go-live"
Tom Cannon	7.16	30/08/23	Simplified the "How to Submit a Change" tables
Tom Cannon	8.0	15/09/23	Change to version numbering, and cleanup of links in the Appendix section.
Tom Cannon	8.01	08/02/24	Minor update to include clarity around PoC and Pilots.