UNIVERSITY OF CALGARY

Information Technologies Change Management Standard

Classification Service Delivery	Table of Contents
Standard # SVD-002	
Approval Authority Chief Information Officer	
Implementation Authority Director, Service Delivery	
Effective Date June 27, 2011	
Latest Revision June 27, 2011	

Definitions **1** **Change**: The addition, modification or removal of anything that could have an effect on IT Services.

Configuration Item (CI): Any technical component (e.g. hardware, software) that needs to be managed in order to deliver an IT Service.

Change Advisory Board (CAB): The governing body that formally authorizes change requests and supports change management processes by providing assistance in assessing and prioritizing change requests. There may be different CABs for different subject areas (e.g. infrastructure, applications, services), but all must conform to this standard.

Emergency Change Advisory Board (ECAB): The governing body that formally authorizes emergency change requests. There may be different ECABs for different subject areas, but all must conform to this standard.

Change Impact: A category used to determine the impact of a change on the organization.

- Major/Widespread
  - Affecting an Institution critical system or
  - Affecting more than 100 users, or an entire system or service, or an entire location, or entire Institution
- Significant/Large
  - Affecting an Institution critical system or
  - Non-Institution critical system or

    - Affecting 20 to 100 users
- Minor/Limited
    - Non-Institution critical system or
    - Affecting 1 to 20 users

Change Urgency: A measure of the severity of the problem to be addressed by the change:

- Severity 1:
    - Response includes an immediate and sustained effort using any and/or all available resources as required until the change is resolved.
    - Hierarchical escalation is invoked, on-call procedures are activated, and vendor support invoked
    - Generally end-users are unable to work and no work around is available
    - Business requires resolution/implementation ASAP
- Severity 2:
    - Assigned team responds immediately, assesses the current situation and may interrupt other staff working lower priority Incidents / Service Requests to assist in timely restoration/implementation of services
    - End-users require expedited restoration/implementation of service, but can bear minimal delays
    - End-users may or may not have a work around available, or workaround may only provide partial relief
    - There is a defined and immediate business deadline
- Severity 3:
    - Assigned team responds using standard procedures and operating within normal supervisory management structures
    - End-users may or may not have a work around available or workaround may only provide partial relief
    - There is an identified business target or deadline
- Severity 4:
    - Assigned team responds using standard procedures and operating within normal supervisory management structures
    - End-users may be inconvenienced, but a suitable workaround is available to allow the end-user to continue working, or a delay in resolution is considered acceptable
    - There is no well-defined or critical deadline identified

Change Priority: A measure of the relative importance of a change. Priority is calculated based on impact and urgency using the prioritization model shown in Table 1.

- **Emergency:** Immediate action is required that does not conform to normal change windows and/or notification periods.
- **High:** Normal change that must be done as soon as possible.
- **Medium:** Normal change with no particular urgency.
- **Low:** Normal change that can wait to be bundled with other changes.

Change Prioritization Model					
		Urgency			
		Severity 1	**Severity 2**	**Severity 3**	**Severity 4**
Impact	**Major/Widespread**	Emergency	High	Medium	Low
	Significant/Large	High	High	Medium	Low
	Minor/Limited	Medium	Medium	Low	Low

Table 1: Change Prioritization Model

Change Classification: Declares the process that the change must follow:

Normal: A change that follows the regular processes and procedures that have been defined.

Emergency: A change that must be introduced as soon as possible.

Standard: A pre-approved change that is low risk, relatively common and follows a procedure.

Standard changes provide agility within the boundaries of change management. The Institution should develop a collection of standard changes, ensuring predictability and the efficient use of resources by using repeatable processes for common change requests. This is accomplished by identifying common recurring changes and optimizing their execution. A standard change begins as a minor, significant, or major change. After the change has been thoroughly tested, deployed, and validated and the execution steps have been documented, a change may become standard.

Change Phase: There are six phases to a change that have various activities and informational requirements. As the change progresses from one phase to another there are various levels of approval required based on the overall risk and nature of the change. The phases are:

Initiate: This phase focuses on gathering the required information and attributes for the change so that expedient decisions can be made in further phases of the change.

Based on the nature of the change, there may be limited information available at the time of initiation. Later stages in the change lifecycle should continuously review the information for completeness and update as required.

Assess: This phase is where the change is examined by the Change Advisory Board (CAB) or Emergency Change Advisory Board (ECAB) to determine any impacts and risks that were not previously identified. Scheduling of the change occurs in this phase.

Build and Test: This phase is where the actual change is designed, built, and tested prior to being moved into production. Testing includes both system level testing as well as User Acceptance Testing (UAT).

Implement: This phase is where the change is moved into production by an authorized change implementer. Changes are tested according to the Post-Test plan and monitored to ensure that the implementation was successful. Should the change fail for any reason then the Back-out Plan is executed. Application and System documentation is updated and made available as required.

Review: This phase is where the net effect of the change is reviewed to ensure that it was successfully implemented and/or to harvest lessons learned.

Close: This phase is the formal closure of the change after it has been reviewed by the relevant stakeholders and all documentation has been updated.

Rationale **2** Change management is very important to the delivery of reliable and effective services and therefore must be planned and purposeful. The University of Calgary relies on change management processes that take into consideration the need for prompt action, reliable service, compliance with policies and alignment with strategic priorities.

Change in any form carries risk—risk of failure, cultural resistance, disruption of operations, technical challenges, resource constraints, and unanticipated consequences.

The Change Management Standard offers best-practice direction to help manage change while addressing risk. An Institution's tolerance and appetite for risk determines the appropriate level of detail and formality to apply to change processes for each type, size, and timing of change.

Configuration Item Asset Management
The primary goal of change management is to create an environment where changes to Configuration Items (CI) can be made with the least amount of risk and impact to the Institution. The Change Management Standard provides rules to achieve the desired outcomes of the change by ensuring repeatable processes are in place for managing changes and to improve reliability and end-user satisfaction.

Sustainable Technology Infrastructure
In order to effectively use technology to enhance the quality of learning and teaching, it must be underpinned by a sustainable technology infrastructure. Sustainability includes the design, construction, planning, and maintenance of an infrastructure that meets the current needs while not compromising those of the future.

Applicability **3** The scope for this Standard includes all changes to any of the information and technology services under the control of the CIO including, but not limited to:

- Technology Infrastructure
- Software and Applications
- Information and Data

Any changes outside the perimeter of information and related technology will be out of scope including, but not limited to:

- Organizational structure and culture
- Business procedure or process
- Information and technology services not under the control of the CIO (i.e. personal laptops)
- Operational tasks that don't affect the technology infrastructure, software or applications, or electronically stored information or data.
- Catastrophes or disasters

Disputes about the applicability of this standard to a particular change will be decided by the Implementation Authority (i.e., the Director of IT Service Delivery).

Standard 4 4.1 Change Request Information Requirements

All change requests must include at least the following information:

- Unique Change Identifier
- Who is requesting the change - Change Requestor
- What is being changed - Configuration Item (CI)
- How is the CI being changed
- Why is the change required
- When is this change requested for
- Documentation of all approvals required in *Table 2* through the lifecycle including who, how, and when
- Current Change Phase (see definition above)
- Change Impact (see definition above)
- Change Urgency (see definition above)
- Business Priority of the change
- Risk Assessment of the change
- Change Classification (see definition above)
- Functional and Non-Functional Requirements of the Change
- Roll-out Plan (Implementation)
- Back-out Plan in case of change failure
- Communication Plan for the change
- Name of who built the change and when
- Pre-Test Plan and Results including who performed the tests
- Name of who implemented the change and when
- Post-Test Plan and Results including who performed the tests
- Name of Post Implementation Reviewer and PIR results (as required)
- Audit trail for all change attributes including:
- Who changed what attributes
- What the value of the attribute was changed to
- When was the attribute changed

If there are multiple individuals acting in a particular role (ie. builder, tester, implementer), all must be listed.

All information must be recorded in such a manner that reports can be generated to satisfy operational, tactical, strategic, and audit requirements.

4.2 Approvals

All changes must be approved at the below listed stages of their life-cycle, as shown in table 2:

Lifecycle Phase Change	Approvals Required
Initiate to Assess	CI Owner
Assess to Build and Test	Impacted Service Owners CAB
Build and Test to Implement	Requester Impacted Service Owners CI Owner UAT Lead CAB
Implement to Review	Requester Impacted Service Owners CI Owner
Review to Close	Requester CAB

Table 2: Change Approval Requirements

Approvals may be delegated provided that the delegation is documented and Segregation of Duties is adhered to.

4.3 Segregation of Duties

Segregation of duties must be practiced to ensure that no single individual has the authority to execute multiple conflicting tasks with potential to impact other systems or information; and that no single individual can execute conflicting end-to-end transactions.

The role of …	Must be independent of …
Requester	Implementer
Builder	Operators of the production environment
Builder	Tester
Builder	Implementer
Builder	At least one approver
Requester	At least one approver
Implementer	At least one approver
Implementer	Reviewer
Auditor	All participants of a specific change
Approver	All other roles listed above

Table 3: Segregation of Duties

Exceptions to Segregation of Duties must be documented and approved by the Change Manager.

4.4 Testing, Communication, and Back-out Plan Requirements

All changes must have testing, communication and back-out plans that are proportionate to the risk and impact of the change and approved by the CAB. The CAB must ensure that all relevant plans are defined and documented to the appropriate level for each change.

4.5 Post Implementation Reviews

The CAB must conduct a Post Implementation Reviews for all changes that fail or have unexpected outcomes so that lessons learned can be applied to future changes.

4.6 Standard Changes

The establishment of Standard Changes must be approved by the Change Manager based on recommendation by the CAB.

Standard changes must be audited on a periodic basis and may revert back to following the Change Management Procedure in the event that the previously tested and validated execution steps have changed or are no longer reliable.

Exceptions **5** The CIO can approve exceptions to the above standard. This authority can be delegated as required.

Exception requests must be submitted to ITASC using the form at http://www.ucalgary.ca/it_files/ea/Request%20for%20Exception%20to%20Standard.pdf, and include:

- a description of exception requested
- the reason for the request
- the impact of the exception being granted or not granted
- for how long the exception will be required and how the need for it will be eliminated
- the compensating controls put in place to maintain the objectives of the standard

Measures **6** The following measures are established to measure how effectively the Change Management Standard has been implemented:

a. Number of exceptions to this standard submitted and approved or rejected
b. Number of non-compliance events, i.e. problems in the change management process itself (missing data, etc.)

c. Number of unauthorized changes detected, i.e. changes implemented that did not follow the appropriate change management process.

Parent Policy **7** **University of Calgary Information Management Policies**

Information Asset Management Policy
Infromation Asset Protection Policy

Provincial Post-Secondary System ITM Control Framework
Technology Management Policy

Related Policies & Standards **8** ***UNIVERSITY OF CALGARY STRATEGIC PRIORITY***
Sustainable Technology Infrastructure

COBIT 4.1
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

ITIL V3
Service Design 3 – Service Design Principles
Service Operation 4 – Service Operation Principles
Service Transition 2 – Service Management as a Practice
Service Transition 3 – Service Transition Principles
Service Transition 4 – Service Transition Processes
Service Transition 5 – Service Transition Common Operation Activities
Service Transition 6 – Organizing for Service Transition
Continual Service Improvement 5 – Continual Service Improvement Methods and Techniques

ISO 27002
6 – Organization of Information Security
8 – Human Resource Security
10 – Communications and Operations Management
11 – Access Control
12 – Information System Acquisition, Development and Maintenance

History **9**

April 29, 2011	Working Group	Initial Draft
June 27, 2011	EASC	Approval