Education

Change management service

Process

Approval

Approved July 2013 by the Information Technology Directorate, Directors Group.

Audience & Applicability

As this policy does not contain process or procedural information, the intended and target audience and applicability is specific to:

- Regional Information Technology Managers;
- Service Management forum;
- Community of Practice;
- Service Delivery Management;
- Service Desk Senior Management;
- SAP Support Centre Management;
- Teaching and Learning Systems Management;
- Learning and Business Support Management.

Context

The policy document has been created to provide a policy and framework to support and underpin a Service Management process within the Service Management organisation. It is not intended to be a process or procedural document and subsequently will be supported by these documents.

Version Control			
Version	**Date**	**Author(s)**	**Details**
V1.0	18/1/2012	Louise Griffin	Updates For publication
V2.0	6/2/2013	Sarah McCulloch	Policy Endorsed by Change Stakeholders
V3.0	23/5/2016	Louise Griffin	Yearly review and updated Policy with Emergency change steps as requested by audit
V3.1	25/5/2018	Louise Griffin	Policy review and update
v3.2	19/06/2019	Louise Griffin	Minor content and formatting updates

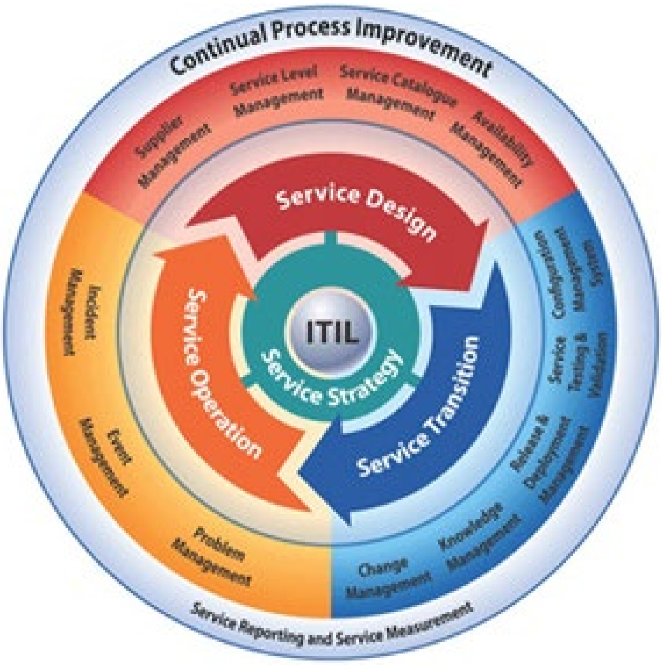
Document Information	
Document Owner	Service Management Office, Change Process Owner
Release Status	Published
Electronic Location	https://education.nsw.gov.au/technology/guides-and-forms/service-management-guides

Contents

Service Management Change Management Policy

1 Introduction

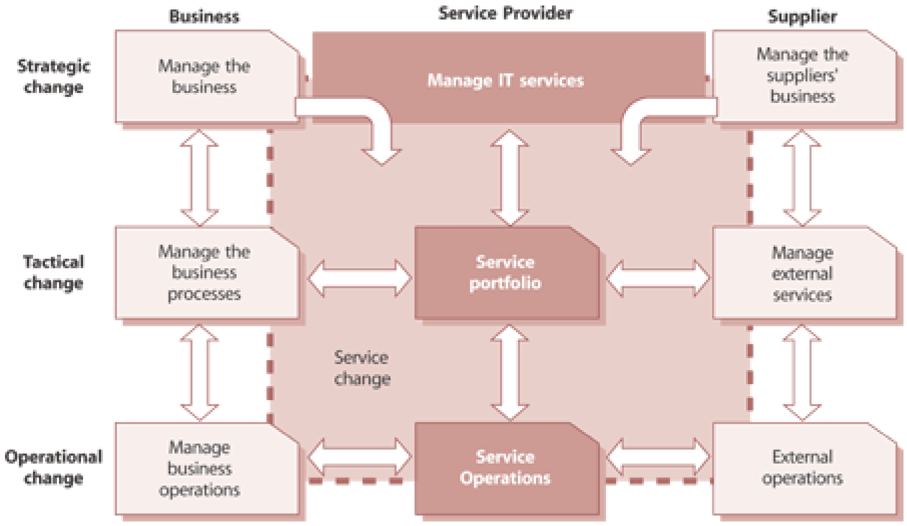
Change management is a significant component of ITIL's Service Operation. Service Operation is the phase of the ITIL Service Management lifecycle that is responsible for "business-as-usual" activities. The following diagram shows Service Operation in relationship to other lifecycle components: Service Strategy, Service Design, Service Transition and Continual Service Improvement.



Within the Service Transition stage of the service lifecycle, Change Management is one of a number of lifecycle processes that impact all lifecycle stages. These processes are:

- Change Management
- Service Asset and Configuration Management
- Knowledge Management.
- Processes focused on Service Transition, but not exclusive to the stage, are:
- Transition Planning and Support
- Release and Deployment Management
- Service Validation and Testing

The following diagram shows a representation of the scope of change management across the key stakeholders from the business consumer to service providers and suppliers



1.1 Purpose

The purpose of Change Management within IT is to ensure that:

- Standardised methods and procedures are used for efficient and prompt handling of all changes.
- Minimising the number of service interruptions resulting from implementation, enhancement and maintenance activities.
- All changes to service assets and configuration items are recorded in the Configuration Management System (as it develops)
- Understand the risk to the business.

Change Management aims to achieve these outcomes through the following means:

- Being a central point of contact for all Change Management activities affecting Service Management Customers.
- Assisting in the resolution of scheduling conflicts
- Setting appropriate lead times to ensure all changes are adequately planned and reviewed
- Increasing visibility within the support community to allow impact assessment across the range of IT services
- Increasing visibility within the Customer base to promote a secure and stable environment
- Providing an efficient review and approval process through the Change Advisory Board

The Service Management Change Management policy document provides clear and comprehensive guidelines for the management of change across the ITD and business units. These policies underpin and guide the functions and activities employed to deliver a quality change management service to the DEC business.

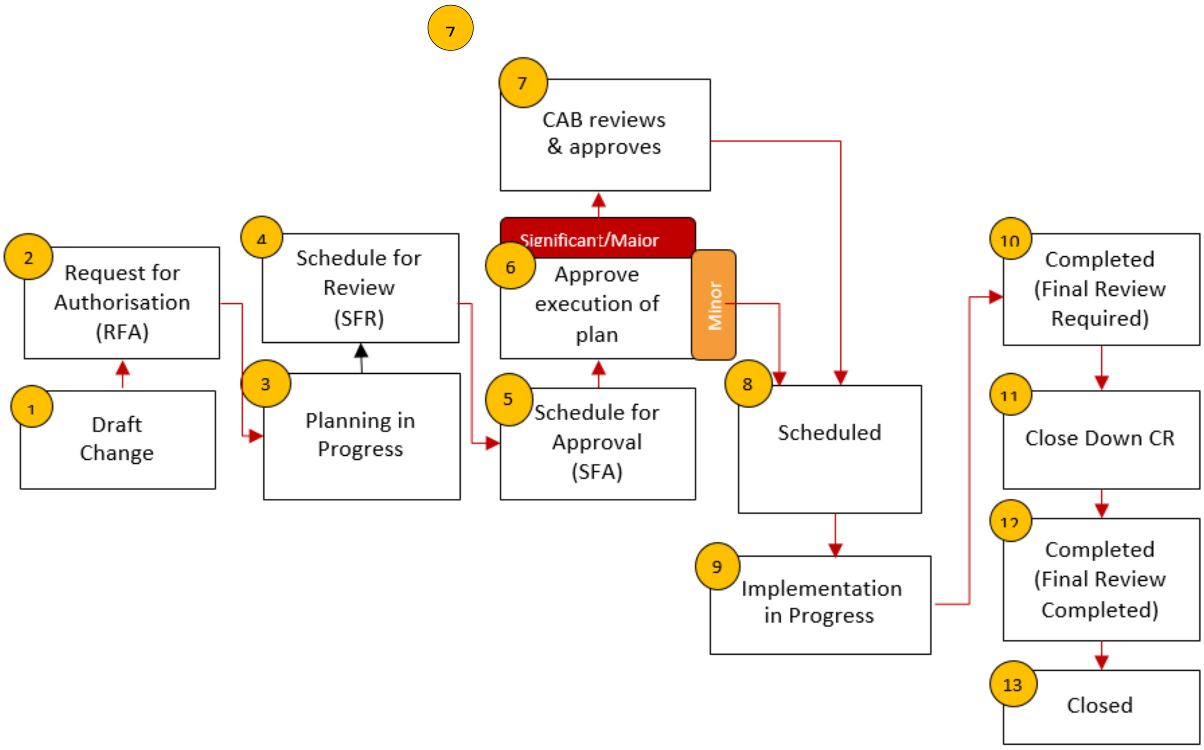
1.2 Change Definition

A change is the addition, modification or removal of an authorised, planned or supported service or service component and its associated documentation.

Change Management ensures that changes are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner.

1.3 Change Process Overview

This section contains a quick reference guide to the key compliance areas of the change management process. In the first instance policy breaches will be reported to the Director.



1) Draft Change Request Creation

2) Request for Authorisation Status (RFA)

3) Planning in Progress includes Risk Assessment and Impact Analysis, Planning and Scheduling of change request to be completed.

4) Schedule for Review Status (SFR)

5) Schedule for Approval Status (SFA)

6) If a change is assessed as SIGNIFICANT or MAJOR impact then refer to CAB for final approval.

7) CAB Approval to proceed

8) Scheduled to Proceed Status

9) Implementation in Progress

10) Completed (Final Review Required)

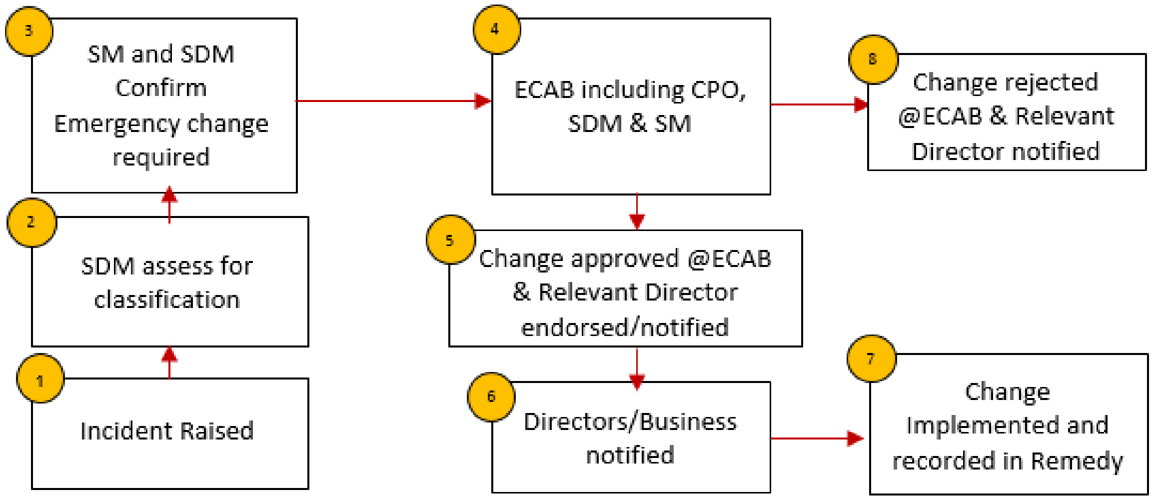
11) Close Change Record

12) Completed (Final Review Completed)

13) Closed

1.4 Emergency Change Process Overview

This section contains a quick reference guide to the key compliance areas of the emergency change management process. In the first instance policy breaches will be reported to the Director.



1) Raise Incident and confirm with Manager

2) Request Service Delivery Manager to review driver to proceed and classify as emergency

3) Senior Manager and Service Delivery Manager confirm emergency change required

4) Senior Manager and Service Delivery Manager request eCAB with Change Process Owner for review

5) Change approved or rejected at eCAB and change progressed through the tool for approval.

6) Director/Business notified of decision of Go decision and change details – timings etc

7) Change Implemented and confirmed successful to fix/remediate the incident.

8) Change rejected at eCAB and relevant Director notified

2 Policy Statements

This policy applies to the management of any change that occurs in relation to a product or service delivered to the Service Management Office (SMO).

The SMO are accountable for ensuring that their respective teams follow the guidelines within this policy statement and the procedures derived from it.

The reason for this policy is to ensure a **Services Thinking Culture**:

A positive customer experience	Because *we plan* and we consider potential *customer impacts and risks* we might be introducing
We minimise service outages	We implement changes within the *agreed business windows to minimise service unavailability*
We provide Quality and Risk assurances	By recording all changes and review quality of plans, quality of data and risk assessment of the intended change
Single source of truth/data	By ensuring all changes are logged in remedy, we can create reports and measure our successes

2.1 Change Windows Policy

Title	Policy
Reason for Policy	1. Change windows are in progress of being established across ITD. 2. The windows are to ensure production stability while minimising the impact of change and 3. reduce outages during working hours.

Policy Statement	ITS Standard monthly change window exists on the third Sunday of every month.
	• Change windows *are flexible* to address *specific requirements and project needs*.
	• Changes required to be *implemented outside of the agreed windows;*
	  o Submit a Change Exemption Form
	  o please refer to the change exemption guidelines
	  o Director level approval will be required for Production environments

	o MAangement level approval will be required for Development envrionments

2.2 Change Type Policy

Title	Policy
Reason for Policy	To ensure rapid resolution and implementation in response to HIO and High Severity incidents. Standard approach to change classification
Policy Statement	**Standard Change** A standard (Pre-approved) change is defined as a change that has an agreed scope and process for implementing the change and does not require approval each time it is implemented. **Normal Change** This defines a Change that requires planning, review, authorisation, scheduling and approval before it can be implemented. These changes progress in accordance with the weekly Change Cycle timeline. Note: The majority of changes go through this process. **Emergency Changes**: require Service Delivery Manager, Change process owner and Senior Management approval. Business to contact their Service Delivery Manager for classification. The classification of an emergency change will be either in response to or prevention of a high or critical outage or incident. Where possible emergency changes are to be raised in the tool at the time. Failing this a retrospective change must be raised and approved 24 hours after the event or by close of business the next working day. The Emergency procedures apply 24 hours per day, 7 days per week Emergency changes are not required to follow the exemption process **Expedited changes**: Changes that are raised outside the required lead-time require justification as to why lead-times are not met and are to be communicated with Change Management. Any critical change that must still go ahead will require a valid justification as to why it didn't meet lead times and why it is critical to go ahead to be included in the change record. **Latent Changes**: Changes that are raised retrospectively once the change has proceeded. Changes will require appropriate approval from management prior to proceeding.

2.3 Change Scheduling Policy

Title	Policy
Reason for Policy	• To ensure all changes comply to the IT Change Methodology. • To ensure consistency in terminology

	• To ensure consistency in the management of changes • To maintain production stability
Policy Statement	**Changes include:** Implementing any Infrastructure and application changes in environments detailed in the process scope. All changes must be submitted for endorsement and fully approved prior to implementation. All changes are to be raised within lead-times All changes are to be endorsed within the stakeholder endorsement time Change records must be closed within 5 days after implementation. This does not affect, nor is affected by, the verification period. If a change failed and/or backed out, the change is to be closed and a new request is to be submitted. All changes implemented by IT that impact Business, must be communicated to Business Representatives at least 5 working days prior to implementation. All changes must contain a minimum content identified in the change tool.

Change Freeze Policy

Title	Policy
Reason for Policy	1. To maintain stability 2. Minimise the risk of further production outages 3. Ensures resources are available for business critical periods for support and BAU activities 4. To minimises disruptions to business
Policy Statement	An IT Change freeze is defined as a period in time where changes may not be implemented into any • development or • production environments An Exemption process can be facilitate any required changes via a governance and management approach.

Title	Policy
	A technical change freeze may be identified into one of three categories: • IT/Business Critical Processing Periods • IT/Business Critical Projects • Unstable Environment

2.4 Change Record Management Policy

For consistency and purity of process, staff with access and training to the change management console will be able to raise changes.

	Change Origin	Description
User Initiated:		
1	Business initiated changes	1. These should be requested via the Service Desk in the form of a Service Request. 2. ITD initiate and manage the required change request record.
2	ITD initiated changes	1. ITD initiate and manage the change.
3	3rd party initiated IT change – for information	2. ITD initiate and manage the change. E.g. network provider outages, building maintenance outages etc.
Incident/Problem Initiated:		
4	Incident or problem initiated changes	3. These should be notified in the form an Incident and/or a Problem. 4. ITD initiate and manage the required change request record.

2.5 Reboot Policy

Title	Policy
Policy Statement	**Summary:** A change record is required for all scheduled reboots. Emergency reboots do not require a change record but do require an incident/problem ticket and a Service Delivery Manager and/or ITD Infrastructure/Application owner approval to proceed. A *scheduled reboot* is a preventative measure for Service Management and IT is based on the history of the environment. Standard reasons for a scheduled reboot are memory leaks and/or thread leaks. A scheduled reboot will also include the following: Monitoring thresholds showing the requirement to reboot to prevent a problem. Reboot is to be scheduled at an appropriate time as a preventative measure and a change record is to be raised and approved by all stakeholders prior to the reboot commencing. Server not required to be rebooted but services required to be stopped and started (potentially part of an application). If an application reboot is required then a ticket number needs to be raised.

	Where multiple scheduled reboots are to occur to prevent an outage whilst root cause is investigated, one of the following two methods can be used: i. Raise a single change record for each reboot. ii. Raise two change records to implement and remove a scheduled reboot procedure. **Note:** the maximum period a scheduled reboot can cover in any one change record is two (2) months. The duration of the change is measured by the time taken to implement the process and remove the process. Any scheduled reboot covered by this process needs to be reported to Change Management. **Emergency Reboots** are in direct response to a system in process of dying or freezing or it has frozen. In all cases where an emergency reboot is required an incident ticket is to be raised and the appropriate manager and or Service Delivery Manager will be contacted for approval prior to rebooting. Exceptions to the above are to be dealt with on a case by case situation in direct communication with Service Management
Reason for Policy	To maintain a stable production environment to support business during business working hours

2.6 Exemption Policy

Title	Policy
Reason for Policy	To maintain a stable production environment to support business.
Policy Statement	1. Directors/Managers to assume *responsibility for the risk* of the release proceeding during freeze periods. 2. Business stakeholder must also approve and assume risk Examples: • Business critical production fixes qualify • Compliance changes required on a specific date which can invoke this process. • Unable to meet release windows for a variety of reasons, could impact other releases/changes • CAB/RAB rejected, Director level endorsement approval can override **All situations will be dealt on a case-by-case situation contact Change Manager.**

2.7 Change Breach Policy

Title	Policy
Reason for Policy	To maintain a stable production environment to support business, studnets, schools and teachers
Policy Statement	Summary: If a change does not follow the documented change policy and process and proceeds without the necessary approval then this is classed as a change breach. In the first instance policy breaches will be reported to the Manager/Director and included in Weekly/Monthly reporting to Senior Management.

3 Glossary

Term	**Definition**
DEC	The New South Wales Department of Education and Communities
ITD	NSW DEC Information Technology Directorate
CM	Change Management
SDM	Service Delivery Manager
ITIL	Information Technology Infrastructure Library
ITM	Information Technology Manager
SM	ITD Senior Manager
Change Window	An agreed pre-organised time when Changes or Releases may be implemented with minimal impact on Services.