



CHANGE MANAGEMENT

Process Definition Document

Abstract

This document defines the Change Management processes in place in Sheridan College's Information Technology department, as part of a larger IT Service Management strategy.

James Duncan
james.duncan@sheridancollege.ca

Acknowledgments

The contribution of the following individuals in preparing this document is gratefully acknowledged:

Role	Name	Phone #	E-Mail Address
Document Owner	James Duncan	2556	james.duncan@sheridancollege.ca
Contributors	Byron Aguilar, Vicken Awakian, John Barber, Waldo Calderon, James Duncan, Paul Khangura, Julia Kraveca, Ausim Mobeen, Samir Muhamedagic, Stan Padacz, Divya Pathak, Usama Pervaiz, Dan Tebbutt, Stuart Tenn		
Reviewer	Julia Kraveca	2123	julia.kraveca@sheridancollege.ca
Approval	Sumon Acharjee	2373	sumon.acharjee@sheridancollege.ca

Document Number	1.4
Document Name	Change Management Process Definition
Date Created (Draft)	2013/12/10
Date Approved	TBD
Document Location	\\adminshare\itprojects\itsm\change management

Version Control

Version	Date	Author	Change Description
0.1	2013/11/11	Julia Kraveca	First template
0.2	2013/11/18	James Duncan	First revision of Roles and Responsibilities section by team
0.3	2013/11/25	James Duncan	Revision of all areas based on subteam meetings
0.4	2013/12/02	James Duncan	Revision of all areas based on subteam meetings
0.5	2013/12/06	James Duncan	Revision of all areas based on subteam meetings, inclusion of CSFs from Waldo
1.0	2013/12/10	James Duncan	Complete first version for review and approval by IT Management Team
1.1	2013/12/11	James Duncan	Adjustments with feedback from IT Management Team - Approved
1.3	2014/05/09	Julia Kraveca	Final review of the document for language consistency and accuracy in aligning to the best practice
1.4	2017/02/08	James Duncan	Minor style changes, update Blackout Period to Special Approvals Period.

Approved:

Sumon Acharjee, CIO (formerly)

Bruce Smith, AVP IT (currently)

Date: 2013/11/12

Table of Contents

- Introduction 6**
- Roles and Responsibilities 6**
 - Change Originator 6
 - Service Owner 6
 - Business Owner 7
 - Change Manager 7
 - Change Advisory Board (CAB) 7
 - IT Management Team 9
- Change Categorization..... 9**
 - Standard Changes..... 9
 - Normal Changes 9
 - Minor Changes 9
 - Significant Changes 10
 - Major Changes 10
 - Emergency Changes 10
- Change Authorization Model..... 11**
- Change Management Schedule 11**
 - Change Window 11
 - Special Approval Periods 11
 - Change Submission Time Frames 12
 - Change Schedule 12
- Request for Change (RFC) 12**
 - Business Reason for the Change 12
 - Implementation Plan 13
 - Test Plan 13
 - Back-out Plan..... 13
 - Impact Assessment..... 13
 - Risk Assessment 15
 - Communications, Training, and Documentation Plan..... 15
 - Change Record States..... 16

Change Management Process Map.....17

Change Management Process Measurements18

 Change Management Reports.....18

 Measurements18

Introduction

This document defines the Change Management process for Sheridan College.

Change management is one of the most important service management processes. Controlling the release of changes allows the management of potential risks and disruptions that changes may bring within them. Change Management's role is to ensure that changes are:

- Documented
- Evaluated
- Planned
- Authorized
- Prioritized
- Tested
- Communicated
- Implemented
- Reviewed

Roles and Responsibilities

Change Originator

The Change Originator is the technical specialist responsible for the planning and implementation of the proposed change. The Change Originator has the following responsibilities with respect to the change management process:

- Create the RFC (Request for Change) which fully documents all aspects of the change
- Completion of assessment activities (business requirements, technical requirements, definition of risk, scope of work, resources required, impact, etc.) of the proposed change using the framework laid out in this Change Management Process document
- Submission of the RFC within appropriate timeframes to meet change approval deadlines
- Discuss the change with the CAB when required
- Be accountable and/or responsible for the successful completion of the change once approved
- Modify the Change Record's status as appropriate

Service Owner

The Service Owner is the primary point of contact for a given service across the organization. This individual has responsibility for decision making, or the escalation of decisions, for all aspects of the service delivery. They are ultimately accountable to the Business Owner for the delivery of the service within the agreed service levels, and for the continual improvement of the service. Often, this individual will lead a team of technical specialists or an internal support unit, accountable to an IT Director.

A service's owner will be defined and maintained as a portion of its entry in a larger Service Catalogue.

The Service Owner has the following responsibilities with respect to the Change Management process:

- Representation of the service in Change Advisory Board meetings
- Assists in the assessment and evaluation of proposed changes affecting their services
- Prepares a review of the change implementation for presentation and discussion with the CAB
- Approves Minor Normal changes
- Closes the change record upon the successful completion of a Minor Normal change

Business Owner

The Business Owner is an individual in the College that is responsible for the definition of business processes or requirements for a given service.

The Service Owner will represent their interests in all Change Management activities. The associated Business Owner could/should be invited to any CAB meetings that discuss significant or major changes to that service.

Change Manager

The Change Manager is a single individual responsible for the promotion, support and management of the Change Management process at Sheridan. This role is accountable to the IT Management Team for the change management process in its entirety.

The Change Manager has the following responsibilities with respect to the Change Management process:

- Chair the Change Advisory Board (CAB)
- Report on the CAB's decisions and recommendations to the IT Management Team
- Provide metrics on change success rates to the IT Management Team
- The Change Manager will escalate decisions to the IT Management Team when CAB is unable to come to a consensus.
- The Change Manager will communicate decisions made around changes by the IT Management Team or the Executive to the CAB

The Change Manager role at Sheridan will be assigned to the Director of Information Technology Support Services. The Change Manager will designate alternate individuals to fill this role in the event that they are unavailable.

Change Advisory Board (CAB)

The Change Advisory Board (CAB) is the body that is responsible for assessing, prioritizing, and authorizing changes that are categorized above a given risk/impact level. The CAB will escalate approval of changes to the IT Management Team when agreement is not reached. Authorization for Minor Normal changes are delegated by the CAB to the Service Owners.

The membership of the CAB should be flexible, depending on the change(s) being reviewed, to ensure that there is proper representation of the appropriate technical and business interests. CAB meetings will be held weekly on Tuesdays at 3pm.

The Change Manager serves as the Chair of the CAB.

The CAB has the following responsibilities with respect to the Change Management process:

- Review changes classified as Significant or Major Normal changes, and approves, denies, or postpones these changes
- Reevaluation of impact and risk assessment where appropriate
- Provide recommendations and feedback with respect to change requests that are denied or postponed
- Review all completed changes against the list of Critical Success Factors documented in this email, and prepares a report for the IT Management Team
- Closure of Significant or Major Change records
- Review requests for classification of changes as a Standard change, and approve or deny these requests
- Recommend improvement opportunities in Change Management

The Change Advisory Board shall consist of the following members:

- Change Manager (Director, Information Technology Support Services)
- Service Owner of any services impacted by proposed changes
- Change Originator of any RFCs currently under discussion (as a guest, to address questions or concerns of the CAB with respect to the change request)
- Business owner(s) of affected services are to be invited as a courtesy but are not required (the Service Owner represents the Business Owners interests in the CAB)
- Other impacted areas (e.g. FAAD, FAST, OTR, HR) as appropriate per each change to be invited as a courtesy
- A Manager or Technical Lead (e.g. Coordinator) from each discrete IT business unit

Emergency Change Advisory Board (ECAB)

The ECAB is a subset of the CAB, also reporting to the Change Manager, which is responsible for authorizing urgent changes. Staff will obtain one approval for all Emergency Changes before they are implemented, escalating as follows until a decision is made:

1. Service Owner responsible for the affected service
2. Director / Manager (or designated backup) accountable for the service
3. IT Crisis Manager on call
4. Change Manager (or designated backup if required)
5. Associate Vice President, Information Technology

IT Management Team

The IT Management Team and/or the AVP-IT serves as the ultimate escalation point for any change management decisions that cannot be resolved by the CAB and/or the Change Manager. The IT Management Team will provide decisions for escalated issues/approvals within 1 business week.

The Change Manager is accountable to the IT Management Team for the change management process, and for the reporting of metrics regarding change successes and failures.

Change Categorization

Proper change categorization is important for an appropriate level of authorization to take place. There can be 3 different types of change requests:

- Standard
- Normal
- Emergency

Standard Changes

Standard changes are well understood, repeatable changes and are pre-authorized. Standard changes have the following characteristics:

- Recurring
- Routine
- Low risk and low impact that is well understood
- Change procedures are already established

Every Standard change must have pre-defined steps to follow for implementation. Each standard change will have had all assessment activities (e.g. risk/impact assessments, technical implementation steps, etc.) completed in advance and documented.

The approval of a previously defined change as a Standard Change is done by the CAB.

Normal Changes

Normal changes follow the complete change management process, and by definition exclude any changes that are approved as Standard changes or would be appropriately classified as an Emergency change.

Normal changes are categorized into 3 classifications based on their assessed impact and risk. Each of these Normal change categories has a unique review and approval workflow associated with it.

Minor Changes

Minor changes have a low assessed risk and impact. They will be approved by the Service Owner and completed outside of a CAB review and approval process.

Significant Changes

Significant changes have a moderate assessed risk and impact. They must be submitted to CAB for approval before completion.

Major Changes

Major changes have a higher degree of assessed risk and/or impact. They must be submitted to CAB for approval before completion, and require a greater amount of scrutiny with respect to their implementation, communication, training etc. requirements. Major changes may be escalated by the CAB to the IT Management team for further review and approval, if necessary.

The following table details how the impact and risk assessment scores defined later in this document are used to categorize a Normal Change as Minor, Significant, or Major:

Risk Score	High	Significant	Major	Major
	Moderate	Minor	Significant	Major
	Low	Minor	Minor	Major
	Low	Moderate	High	
	Impact Score			

Emergency Changes

An emergency change is implemented to repair an IT service due to an issue that has a high degree of impact on the business, or to protect the organization from a threat. Normal changes not submitted on time will not be treated as emergency changes.

Emergency changes must be logged, and are subject to defined communications and/or incident management processes that must be followed.

Emergency Changes must be approved by the identified ECAB escalation process, and will be recorded within 2 business days of the implementation of the change by the Change Originator.

Change Authorization Model

The following table summarizes the level of approval required for each of the above change classifications:

Change Type	Change Authority
Standard Change	Pre-approved by Change Advisory Board (CAB)
Normal Changes	
Minor Change	Service Owner
Significant Change	Change Advisory Board (CAB)
Major Change	Change Advisory Board (CAB)
Emergency Changes	Emergency Change Advisory Board (ECAB)

Change Management Schedule

Changes will be scheduled in a way that it meets business needs rather than IT needs. This means that changes will be scheduled within pre-established windows appropriate to the services impacted by the change, and respecting other timelines laid out in this document.

Change Window

A change window is defined as a period of time during which changes to services can be implemented with minimal impact to business operations.

Change windows will be defined for each service appropriate to the risk and the impact of a change on business operations. The change windows should be documented in a Service Level Agreement (SLA) with the following minimum information:

- Service Name
- Change Category (e.g. Standard, Minor/Significant/Major Normal, etc.)
- Change Window for each category above

The 3rd Sunday of each month is reserved as a static and predictable change window for large and potentially disruptive changes.

Special Approval Periods

During these time periods, all Normal changes must be logged in advance and approved at CAB.

The following Special Approval periods will be observed at Sheridan:

- Fall term startup: 2 full calendar weeks before the start of term to 2 full calendar weeks after the start of term

- Winter term startup: 3 full calendar weeks before the start of term until 1 full calendar week after the start of term
- Summer term: 2 full calendar weeks before the start of term until 1 full calendar week after the start of term

Change Submission Time Frames

Normal change requests must be submitted a minimum of 3 business days prior to the next CAB meeting if they require the review and approval of that group. Requests for Change (RFCs) received after this time period will be deferred until the next CAB meeting. This time period is required so that affected areas can review the change and ask questions or raise concerns with the Service Owner / Change Originator in advance. The Change Manager has sole discretion over the adjustment of change submission windows.

Minor change requests will be reviewed by the Service Owner within a maximum of two business days.

Change records for emergency changes must be logged within 2 business days of the completion of the change.

Change Schedule

A list of all proposed and approved changes and their implementation dates will be recorded in a Change Schedule that is publicly available.

Request for Change (RFC)

Changes are documented throughout their lifecycle as a Request for Change (RFC). The RFC will provide the following information to allow the Service Owner and/or Change Advisory Board to assess the proposed change. The RFC will consist of several components:

1. Reason for the change
2. Technical details of the change
3. A plan to test the change after implementation
4. A plan to reverse all or part of the change if required
5. Impact and risk assessment of the change (used to categorize the change for approval processes)
6. Proposed communications and support plan

Business Reason for the Change

This section of the RFC provides definition around the reason for the change, and should answer the following questions:

1. Who raised the change?
2. What is the reason for the change?
3. What is the return required from the change?

Implementation Plan

The RFC will contain technical specifics to a degree of detail appropriate for other subject matter experts to fully understand – and, if required, implement – the proposed change. This section should answer the following questions:

1. What steps are required to implement the change?
2. What resources (people, software, hardware, etc.) are required to deliver the change?
3. Who is responsible for the implementation of the change?
4. What is the relationship between this change and other changes (e.g. interdependencies between changes)?
5. When is the change proposed to occur?

Test Plan

The RFC will contain a plan for testing the change after implementation, and identify the resources required to perform that testing.

Back-out Plan

A back-out plan is a documented set of steps or actions that are to be taken to restore the service if the change fails or partially fails. The back-out plan may account for the reversal of the entire change or a subset of the change as appropriate.

The RFC must include a back-out plan to be reviewed by the Service Owner and/or CAB before approving the change.

Impact Assessment

To facilitate the impact assessment the following questionnaire must be completed by the Change Originator.

Question	Weight	Options (scored from 1 to 5)				
Who is impacted by the change?	3	Individual	Office or entire class	Wing / Building, OR Academic program, OR Department	Campus-wide	College-wide
What is the impact on business operations?	3	No / very little impact on business operation	Minor impact with workaround identified	Significant impact with no workaround	Permanent change to business process	Service unavailable
What is the effect on customer service? (training, documentation, ongoing resource requirements)	1	No effect / little effect	Minor effect	Significant effect	Considerable effect	Major changes to one or more areas of customer service
What is the effect on other services or infrastructure?	2	No effect	Minor impact on department or an individual	Significant impact on other business critical services	Considerable impact on other mission critical services?	Major impact on other mission critical services
What is the duration of the identified impact to the business?	1	No outage or permanent change	Less than 5 minutes	Between 5 and 15 minutes	Between 15 minutes and 1 hour	More than 1 hour
What is the effect of not implementing the change?	2	No effect, business as usual	Lack of service optimization (cannot introduce new functionality, etc.)	Cost avoidance opportunity is missed	There is a risk to existing infrastructure, OR An existing issue will not be resolved, OR Change is a key deliverable in an active project.	Compliance issue, OR Reputation of college could be significantly impacted.

Each answer maps to a score from 1 to 5 (in order of least impactful to most impactful) which is then multiplied by the question’s weighting. The sum of the scores for all questions is then evaluated against the following table to determine the change’s impact:

Assessment Score	Change Impact Evaluation
40 to 60	High Impact – change must be evaluated by CAB
25 to 40	Moderate Impact – change must be evaluated by CAB or SO depending on risk
12 to 25	Low Impact – change must be evaluated by CAB or SO depending on risk

Risk Assessment

ITIL best practices remind us that “No change is without risk”. Risk assessment is one of the mandatory activities that must be performed before change categorization. It is required to use the below risk assessment matrix to assign an appropriate risk level to the proposed change request. The risk assessment process is built into the overall change assessment workflow.

<p>Severity</p> <p>On a scale of 1 to 5, what is the potential impact to the effective operation of a service if an issue occurs with the change.</p> <p>The severity rating can be mitigated by an effective and tested roll-back plan.</p>	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
<p>Probability</p> <p>On a scale of 1 to 5, what is the likelihood that a problem may occur with a given change? (1 = extremely unlikely, 5 = almost certain)</p>					

Risk Score	Action
20-25 High Risk	Change is very risky and should be evaluated by CAB
10-20 Moderate Risk	Change is moderately risky and should be evaluated by CAB
1-10 Low Risk	Change is very low risk and must be approved by Service Owner at a minimum

Communications, Training, and Documentation Plan

The RFC will detail the communications, documentation, and training requirements for the proposed change, taking into account all appropriate stakeholders of the service (within and outside Information Technology).

The Service Owner and/or CAB will review – and if necessary, modify – the proposed communications plan.

The proposed plan should take into account the following factors (some of which will have been identified during the impact assessment):

- Who is affected by the proposed change? (both inside Information Technology, and otherwise)
- What is the impact of the change on these people?
- What are the appropriate tools to communicate the change to everyone affected?
- What is the amount of notice required for the proposed change?
- What are the implications of the change on Information Technology Support Services?
- Does existing documentation have to be updated, or does new documentation have to be prepared?
- Does Information Technology staff members, or users of the service, require training related to the change?

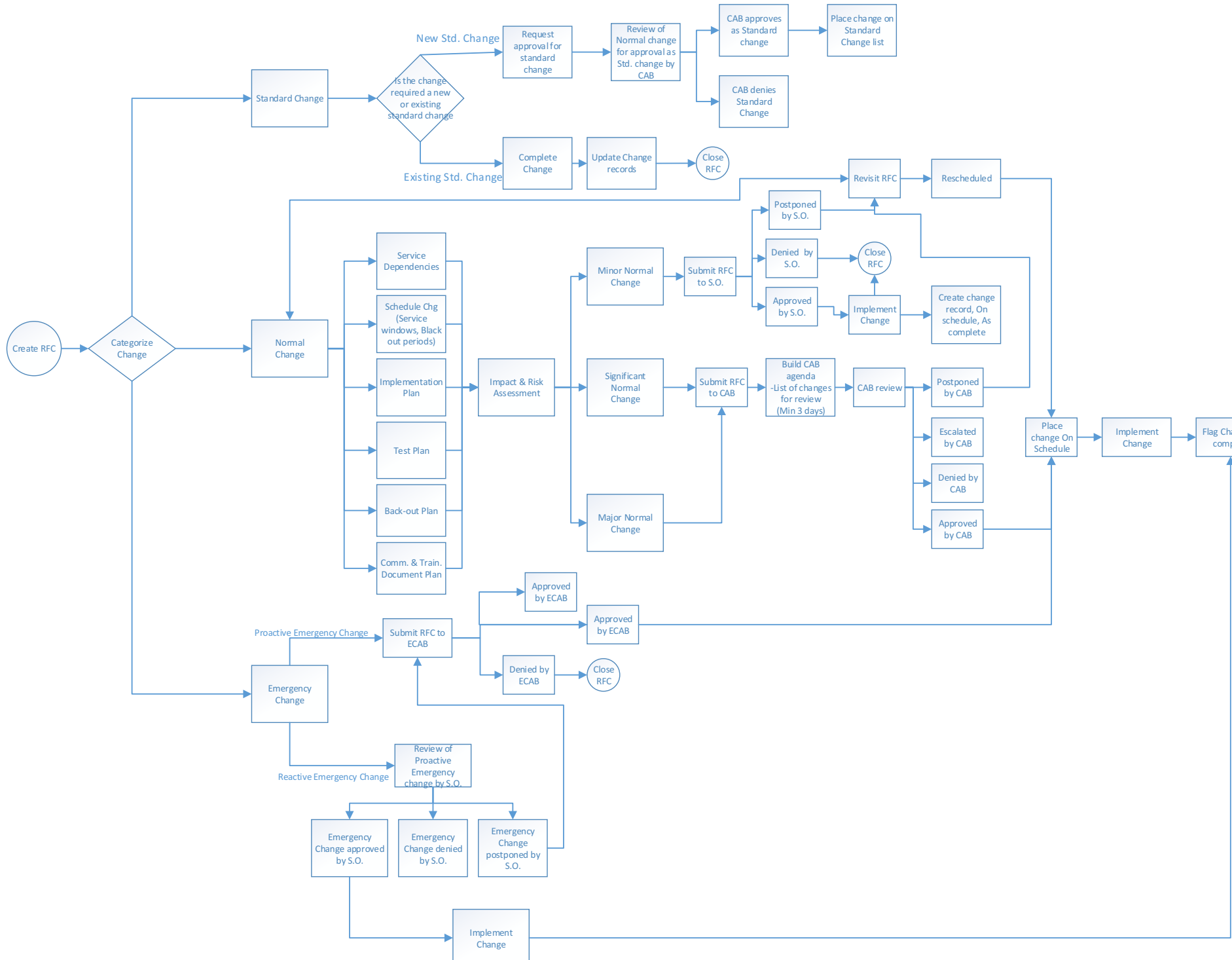
Change Record States

The RFC state will be modified by various individuals/groups during the lifecycle of the change where appropriate:

State	Description	Modifying Authority
Draft	An RFC begins in this state until it is ready for review by the appropriate approval authority ('Proposed')	Default State – Change Originator
Proposed	The RFC is ready for review/approval	Change Originator
Approved	The RFC is approved for implementation	Service Owner or CAB (based on change classification)
Postponed	The RFC requires rescheduling or further updates before it can be approved	Service Owner or CAB (based on change classification)
Rejected	The RFC is not approved for implementation	Service Owner or CAB (based on change classification)
Complete	The change was completed	Change Originator
Incomplete	The change was not completed or is not fully complete	Change Originator
Closed	The change has been reviewed by CAB and/or the Service Owner and requires no further work.	CAB or Service Owner

Change Management Process Map

The following diagram describes the overall workflow of changes from their proposed state through to the closure of the change record (note – this requires fu



Change Management Process Measurements

Change Management Reports

Reports will be developed and presented to the IT Management Team on the success rate of change implementations, number of tickets generated as a result of changes, aggregate information about changes, etc.

Measurements

The following Critical Success Factors (CSFs) will be evaluated over time and analyzed by the CAB for recommendations to the IT Management Team on required Change Management process improvements:

CSF #1 (Protect Services When Making Changes)

- Reduction in the number and percentage of changes with incomplete/inaccurate impact assessments
- Reduction in the number of incidents attributed to approved changes
- Reduction in the percentage of changes that are categorized as emergency
- Reduction in service unavailability due to changes
- Was change executed on time and within the projected service outage period?

CSF #2 (Ensure all changes to components are well managed and recorded in a timely manner)

- Reduction in number and percentage of compliance issues (e.g. procedures were not followed) for the Change Management process
- Reduction in number and percentage of incomplete change records
- Reduction in number and percentage of incomplete status updates of change records
- Increase in the accuracy of all documentation of assets, components, systems, and services

CSF #3 (Optimize overall risk)

- Reduction in the percentage of changes that are categorized as emergency
- Increase in number and percentage of documented testing
- Increase in number and percentage of documented risk/impact analysis
- Was the change completed successfully?
- Reduction of unsuccessful changes
- Reduction of disruption to services due to planned or unplanned changes
- Was risk assessment accurate and complete?

CSF #4 (Increase customer satisfaction of the Sheridan Community with IT services)

- Increase satisfaction of the Sheridan Community with IT services
- Did the change meet or exceed the customer requirements
- Decrease the amount of changes not communicated to Sheridan Community.