



**Change Management  
Environments, Policies & Procedures**

**Version: 01.00.00**

May 15, 2007

**Clemson University  
Office of the Vice Provost and CIO  
Computing and Information Technology**

<b>1.0 Introduction.....</b>	<b>4</b>
<b>2.0 Purpose.....</b>	<b>4</b>
<b>3.0 Scope.....</b>	<b>4</b>
<b>4.0 Change Management Concepts.....</b>	<b>5</b>
<b>4.1 The definition of Change.....</b>	<b>5</b>
<b>4.2 The definition of Change Management .....</b>	<b>5</b>
<b>4.3 The Major Phases of Change Management .....</b>	<b>6</b>
<b>4.4 Change Management vs. Project Change Management .....</b>	<b>6</b>
<b>4.5 Requests for Change (RFC) vs. Request for Service (RFS).....</b>	<b>7</b>
<b>4.6 Request for Change (RFC) .....</b>	<b>7</b>
<b>4.7 Release Planning .....</b>	<b>8</b>
<b>4.8 Change Logs.....</b>	<b>8</b>
<b>4.9 Change Metrics .....</b>	<b>9</b>
<b>4.10 Forward Schedule of Change .....</b>	<b>9</b>
<b>4.11 Critical Outage.....</b>	<b>9</b>
<b>5.0 Change Management Structure .....</b>	<b>10</b>
<b>6.0 Roles and Responsibilities .....</b>	<b>11</b>
<b>6.1 The CCIT Change Manager.....</b>	<b>11</b>
<b>6.2 The CCIT Change Advisory Board .....</b>	<b>12</b>
<b>6.3 Change Governance Board.....</b>	<b>13</b>
<b>6.4 Divisional Change Coordinator.....</b>	<b>14</b>
<b>6.4 Divisional Change Advisory Boards .....</b>	<b>15</b>
<b>6.4 Change Initiator.....</b>	<b>15</b>
<b>6.5 Change Owner .....</b>	<b>15</b>
<b>7.0 The Change Management Process – 8 Steps .....</b>	<b>15</b>
<b>7.1 Logging .....</b>	<b>18</b>
<b>7.2 Filtering .....</b>	<b>18</b>
<b>7.3 Categorization.....</b>	<b>18</b>
<b>7.4 Assessment.....</b>	<b>23</b>
<b>7.5 Authorization .....</b>	<b>24</b>
<b>7.6 Scheduling .....</b>	<b>24</b>

<b>7.7 Implementation</b> .....	<b>27</b>
<b>7.8 Review</b> .....	<b>27</b>
<b>7.9 Change Management Meetings</b> .....	<b>28</b>
<b>8.0 Reviewing the Change Management program for Efficiency and Effectiveness</b> .....	<b>28</b>
<b>9.0 Benefits, Costs, and Possible Problems</b> .....	<b>29</b>
<b>9.1 Benefits</b> .....	<b>29</b>
<b>9.2 Costs</b> .....	<b>29</b>
<b>9.3 Possible problems</b> .....	<b>30</b>
<b>Glossary</b> .....	<b>32</b>

## 1.0 Introduction

A major challenge within any organization is the ability to manage change. This process is even more difficult within an IT organization. Hundreds, if not thousands, of servers, software applications, databases, networking equipment and ancillary devices result in an environment difficult, if not nearly impossible to manage.

The challenge to the organization is not so much maintaining the environment, rather in managing the changes involved in that maintenance. Establishing a process to manage all changes within an environment is so difficult not many organizations can effectively do it.

Making changes to the components comprising an IT system most often stem from the need to improve that service. The reasons for improving a service arise from the need to correct a problem, implement an enhancement that will improve service quality, or implement a change that will reduce service costs. The challenge is to implement a system change that achieves the reason for the change without jeopardizing the integrity of that system or service.

Effective change to IT Systems requires a Change Management program that addresses the risks, business continuity issues, impact, resource requirements, benefits, communication requirements, approvals, and implementation plans associated with the change.

The objective of this document is to define the Change Management program and processes for the Department of Clemson Computing and Information Technology (CCIT) at Clemson University. The Change Management processes presented in this document are based on the Information Technology Infrastructure Library (ITIL) methodology for IT Service Management best practices.

The goal of the CCIT Change Management program is to:

*Ensure standardized methods and procedures are used for efficient and prompt handling of all changes to IT Systems, in order to minimize disruptions to service delivery, improve service quality, and reduce service delivery costs.*

## 2.0 Purpose

This document is provided to define the environment, processes and policies regarding the implementation and use of a Change Management Program for the Department of Computing and Information Technology.

## 3.0 Scope

The policies and procedures identified within this document are applicable to all units within the Department of Computing and Information Technology at Clemson University. All units and areas of the organization will participate in the change management procedures outlined including the documentation of all changes within the CCIT system environments.

## 4.0 Change Management Concepts

This section describes general concepts and definitions associated with the Change Management process. It contains the definitions of Change, Change Management, Request for Service and Request for Change, as well as descriptions of the Major Phases of Change Management, the difference between project change control and Change Management, release planning, change logs, change metrics, Forward Schedule of Changes and critical outage planning.

### 4.1 The definition of Change

For the purposes of this document, Change is defined as:

*The addition, modification, or removal of approved and supported production hardware, firmware, software, applications, facilities, systems, services or associated documentation that support an IT Service or System.*

An IT System consists of integrated production systems (hardware, applications, documentation, training, customer support, consultation, etc) that deliver value to the IT Customer per the Customer's expectation.

### 4.2 The definition of Change Management

Change Management is defined as:

*The process of controlling IT System changes in a manner that assures minimal disruption in service delivery or degradation in service quality.*

The Change Management process, in general, is responsible for controlling alterations to IT components that comprise an IT system and typically encompass the following major areas:

- physical facilities
- hardware
- communications equipment
- applications
- documentation
- customer support
- training
- procedures
- policy

While the Change Management process provides the mechanism for approving (or denying), proposed Changes, the decision authority for approving changes lies with the Change Manager. In order to make sound decisions, the Change Manager relies on input from the Change Advisory Board (CAB) and any other reliable sources of information.

As its name implies, the Change Advisory Board (CAB) functions in an advisory capacity to the Change Manager and, in turn, to CCIT. The CAB is comprised of at least one representative from each division within CCIT, and at-large members representing major customer groups – such as Colleges, Business Services and Student Services. The Change Manager is a staff role within CCIT, while the members of the CAB are appointed by the Executive Directors of the individual divisions within CCIT.

The Change Management process within CCIT is designed to be a hierarchical process with Divisional programs supporting the CCIT Change Management program. Established Change Advisory Boards for each Division should manage all changes within their respective areas supporting IT Services. Approved changes within divisional Change Management programs that will impact other divisions of CCIT or the production systems provided to customers, will be escalated to the CCIT Change Manager and CCIT CAB for review and approval. The goal is not to duplicate the Change process but to keep local changes in local control, so as not to overwhelm the broader mission of the CCIT Change Manager and CAB.

### **4.3 The Major Phases of Change Management**

Managing Change requires a commitment from management to reduce risk exposure and the severity of disruptions, thereby improving service quality and increasing customer satisfaction. The fundamental activities of Change Management consist of planning, controlling, managing risk, minimizing disruption, communicating, implementing, and measuring change. The Change Management process consists of three primary phases. They are:

#### **1. Collect Inputs:**

- Process RFCs (Requests for Change)
- Process FSCs (Forward Schedule of Changes, i.e. a calendar of planned changes)

#### **2. Manage Activities:**

- Filter RFCs
- Manage Change requests
- Manage the Change process
- Chair the CAB (Change Advisory Board)
- Chair the CAB Emergency Committee
- Review RFCs
- Close RFCs
- General administration

#### **3. Produce Outputs:**

- Report FSC status
- Report RFCs status
- Publish CAB minutes and actions
- Publish Change Management reports

### **4.4 Change Management vs. Project Change Management**

Changes to IT elements that are part of a development project - applications, hardware, documentation, or procedures - are not under the jurisdiction of the IT Change Management process. They are, however, subject to Project Management change procedures. Project Managers are expected to work closely with the IT Change Manager to ensure smooth implementation of project outputs into the production

environment. This coordination is handled through the Production Certification portion of Change Management.

#### 4.5 Requests for Change (RFC) vs. Request for Service (RFS)

It is essential to understand the difference between a Request for Change (RFC) and a Request for Service (RFS). Many organizations misclassify Requests for Service as Requests for Change which results in an over-burdened Change process. In general, Requests for Service are procedural (low risk) and often handled by the Service Desk.

A **Request for Service** is characterized as:

*a Change that can be made under strict, well defined procedural control and is therefore (virtually) risk free.*

Providing computer access for a new employee, installing a telephone, replacing a damaged piece of equipment, or resetting a users password are examples of a Request for Service (RFS). They all follow a well defined procedural control.

In contrast, a **Request for Change** can be characterized as:

*a proposed Change to any component of the IT infrastructure or any aspect of an IT system where the proposed Change **could adversely impact service delivery.***

Upgrading a production server, reconfiguring a Local Area Network (LAN), or changing the procedure for changing passwords are all examples of a Request for Change as there is inherent risk to the integrity of production environment components and the systems they support.

#### 4.6 Request for Change (RFC)

Requests for Change (RFCs) are triggered for a wide variety of reasons, from a wide variety of sources that include:

- required resolution of an Incident or Problem report
- User or Customer dissatisfaction expressed via Customer liaison or Service Level Management
- a proposed upgrade to some component of the infrastructure (hardware, software, Service Level Agreement, application)
- changed business requirements or direction
- new or changed legislation
- location change
- product or service changes.

Requests for Change can be concerned with any part of the infrastructure or with any service or activity. Some examples include:

- hardware
- software
- documentation
- telecommunications facilities
- data network

- training courses
- IT infrastructure management procedures
- tactical plans
- environmental infrastructure.

The following items should be included in an RFC form, whether paper or electronic:

- RFC number (plus cross reference to Problem report number, as applicable)
- description and identity of item(s) to be changed
- reason for Change
- effect of not implementing the Change
- version of item to be changed
- name, location and telephone number of person proposing the Change
- date the Change is proposed
- Change priority
- impact and resource assessment (which may be on separate forms where convenient)
- CAB recommendations where appropriate (which may be held separately, with impact and resource assessments, where convenient)
- authorization signature (could be electronic)
- authorized date and time of change implementation
- location of Release/implementation plan
- details of Change builder/implementer
- back-out plan
- actual implementation date and time
- review date
- review results (including cross-reference to new RFC where necessary)
- risk assessment and management
- impact on business continuity and contingency plans
- status of RFC - i.e. 'requested', 'assessed', 'rejected', 'accepted', 'scheduled', 'implemented'.

#### **4.7 Release Planning**

A Release plan should be provided for all but the simplest of Changes and it should document how to back out from the Change, should it fail. On completion of the Change, the results should be reported for assessment to those responsible for managing Changes, and then presented as a completed Change for Customer agreement (including the closing of related Incidents, Problems or Known Errors). For major Changes, Customer input should be solicited throughout the entire process. However, the Customer should always be considered before any Change is implemented.

#### **4.8 Change Logs**

As the Change proceeds through its life-cycle, the Change Request and the Change log should be updated, so the person whom initiated the Change is aware of its status. Actual resources used and the costs incurred should be recorded as part of the record. An After Action Review (AAR) should be carried out to confirm that the Change has met its objectives, Customers are satisfied with the results; and there have been no unexpected side-effects. Lessons learned should be fed back into future Changes. Small

organizations may opt to use spot checking of Changes rather than large-scale AAR's; in larger organizations, spot-checking will have a value when there are many similar Changes taking place.

## **4.9 Change Metrics**

The Change Manager establishes measurements that have *specific* meaning. While it is relatively easy to count the number of Incidents that become Problems that become Changes, it is more valuable to determine the underlying cause of Changes, and to identify trends. Better still to be able to measure the impact of Changes and to demonstrate reduced disruption over time because of the introduction of Change Management, and also to measure the speed and effectiveness with which the IT infrastructure responds to identified business needs. Measures taken should be linked to business goals wherever practical - and to cost, service availability, and reliability. Any predictions should be compared with actual measurements.

## **4.10 Forward Schedule of Change**

Scheduling Changes for implementation should meet business schedules rather than IT schedules. In order to facilitate this, Change Management should coordinate the production and distribution of a Forward Schedule of Changes (FSC) and Projected Service Availability (PSA) report. These documents should be available to everyone within the IT organization, as well as its customers.

The Forward Schedule of Changes (FSC) contains details of all the Changes approved for implementation and their proposed implementation dates. The Projected Service Availability (PSA) report contains details of Changes to agreed Service Level Agreements (SLAs) and service availability because of the currently planned Forward Schedule of Changes (FSC).

These documents should be agreed upon with the relevant Customers within the business, with Service Level Management, and with the Service Desk. Once agreed, the University Operations Center (UOC) should communicate any planned additional downtime to the User community at large, using the CCIT System Notification System.

By planning a Change using schedules to support implementation plans, it is possible to predict the impact of the Change. By examining the records of similar prior implementations (lessons learned) the certainty level of current predictions can be improved and help ensure that the Change will proceed smoothly.

## **4.11 Critical Outage**

Although planning for the recovery of critical business systems is not a task that is the direct responsibility of Change Management, its involvement is essential. This is because any plans to recover IT systems and services that are fundamental to the business will be subject to Change and should be controlled to ensure smooth operation.

It is also necessary to consider what should be done in the event of the plans going awry - or even if you need to back out from Changes resulting from use of the plans. In these instances, the previously mentioned advice about planning for back-outs very early in the planning phase becomes particularly important.

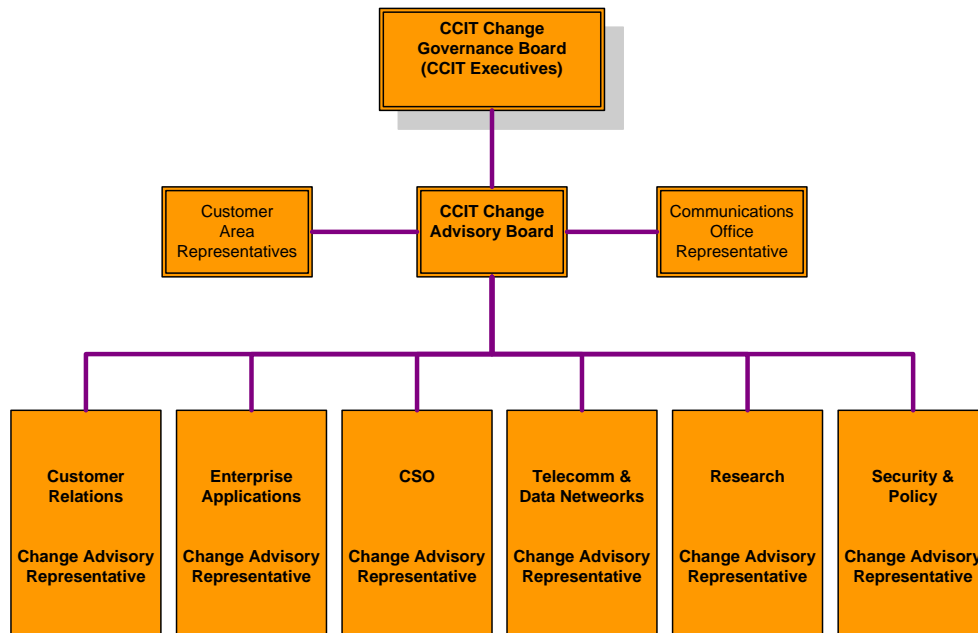
## 5.0 Change Management Structure

This section describes the organizational structure of CCIT's Change Management programs within each division and for the overall department. Defined are the Divisional CAB's, CCIT CAB, CCIT CGB (Change Governance Board) and the connection between the environments.

As discussed in section 4.2, the CCIT Change Management Program is designed to be of a hierarchical nature. Divisional Change Management programs should be established to review RFC's for all changes, regardless of environment type; e.g. Production, Testing, Training, Q&A, Development or Research. Changes that do not affect the Production environments or Customers are tracked, approved, managed and scheduled at the Division level.

Any RFC that pertains to Production environments or impact customers in any way are identified, tracked and escalated to the CCIT Change Management CAB for review and approval. At this point RFC's are approved for implementation, denied (due to scheduling issues) or escalated to the Change Governance Board for Senior Management authorization.

The Divisional programs will mirror that in place for CCIT but, concerned only with RFC's pertaining to those areas assigned to the Division.



The CCIT Change Management Program is the responsibility of the Vice-President for Information Technology. The management and oversight of this program is assigned to the Computing, Systems and Operations Division (CSO), with the Director of Operations appointed as the Director over CCIT Change Management. With the Operations area of CCIT being responsible for monitoring and overseeing the production environment of CCIT services, this delegation of responsibilities allows the University Operations Center, Production Control and

Data Center Facilities areas to document and communicate changes within, and those affecting CCIT's services and environments.

## **6.0 Roles and Responsibilities**

This section describes the major roles and responsibilities associated with the Change Management process. It contains the descriptions of the Change Manager, Change Advisory Board, Change Governance Board, Change Initiator and the Change Owner.

### **6.1 The CCIT Change Manager**

The Change Manager is ultimately responsible for the integrity of the Change Process and is the sole authority for approving Requests for Change. It is an important role for the organization that requires excellent organization, communications, negotiation, analytical decision making, and leadership skills. The Change Manager chairs the Change Advisory Board (CAB) meetings and has the authority to call Emergency Change (CAB/EC) meetings in the case of an emergency IT event that requires immediate action, as well as convene the Change Governance Board for those Changes of a more significant magnitude. A list of responsibilities for the Change Manager role is outlined below:

- Receive, log and allocate a priority, in collaboration with the initiator, to all RFCs. Reject any RFCs that are totally impractical.
- Present all RFCs at a CAB meeting, issue an agenda and circulate all RFCs to CAB members in advance of meetings to allow prior consideration.
- Convene urgent CAB or CGB/EC meetings for all urgent RFCs.
- Chair all CAB and CGB/EC meetings.
- After consideration of the advice given by the CAB or CGB/EC, authorize acceptable Changes.
- Convene Change Governance Board (CGB) meetings for large-scale changes requiring senior management involvement.
- Chair CGB meetings, and after consultation render decision on requested Change.
- Issue FSCs, via the University Operations Center (UOC).
- Liaise with all necessary parties to coordinate Change building, testing and implementation, in accordance with schedules.
- Update the Change log with all progress that occurs, including any actions to correct problems and/or to take opportunities to improve service quality.
- Review all implemented Changes to ensure they have met their objectives. Refer back any that have been backed out or have failed.
- Review all outstanding RFCs awaiting consideration or awaiting action.
- Analyze Change records to determine any trends or apparent problems that occur. Seek resolution with relevant parties.
- Close RFCs.
- Produce regular and accurate management reports.
- Represent divisional and customer interests as a member of the CCIT CAB and CAB/EC

## 6.2 The CCIT Change Advisory Board

The CCIT Change Advisory Board (CAB) is a body that exists to assess and provide input to the Change Manager in the assessment and prioritization of Changes. When a CAB is established, its appointed members should be personnel capable of ensuring that all Changes are adequately assessed from both a business and a technical viewpoint. To achieve this mix, the CAB should include personnel with a clear understanding of the customer business needs and the user community, as well as the technical development and support functions.

The CAB membership should be comprised of:

- The CCIT Change Manager
- A representative from each CCIT division and/or major administrative group, preferably the Divisional Service Management representative
- A Business Services representative
- A Student Services representative
- Clemson University College Representatives
- and may include:
  - applications developers/maintainers (where appropriate)
  - experts/technical consultants (as needed)
  - services staff (as required)
  - facility staff (where Changes may affect accommodation and vice versa)
  - Contractors or third party representatives (as required - for instances of outsourcing situations).

The main duties of the CCIT CAB member are:

- Review all submitted RFCs. As appropriate, determine and provide details of their likely impact, the implementation resources, and the ongoing costs of all Changes
- Attend all CAB meetings. Consider all Changes on the agenda and provide input on which Changes should be authorized
- Participate in the scheduling of all Changes
- Be available for consultation should an Emergency or Urgent Change be required
- Provide advice to the Change Manager on aspects of proposed Emergency or Urgent Changes

CAB meetings represent a potentially large overhead on the time of members. Therefore all RFCs, together with the FSC and the PSA, should be circulated in advance. Relevant papers should be circulated in advance to allow CAB members (and others who are required by Change Management or CAB members) to conduct impact and resource assessments.

In some circumstances it will be desirable to table RFCs at one CAB meeting for more detailed explanation or clarification before CAB members take the papers away for consideration, in time for the next meeting.

A typical CAB agenda should include a review of:

- failed Changes, backed-out Changes, or Changes applied without reference to the CAB by Incident Management, Problem Management or Change Management
- RFCs to be assessed by CAB members
- RFCs that have been assessed by CAB members

- Change reviews
- the Change Management process, including any amendments made to it during the period under discussion, as well as proposed Changes
- Change Management accomplishments or failures for the period under discussion, i.e. a review of the business benefits accrued by way of the Change Management process.

When conducting the impact and resource assessment for RFCs referred to them, the CAB should consider the following items:

- the impact the Change will have upon the customer's business operation in accordance with the Critical Dates Calendar
- the effect upon the infrastructure and Customer Service, as defined in the SLA, and upon the impact on capacity and performance, reliability and resilience, contingency plans, and security of the service
- the impact on other services that run on the same infrastructure (or on software development projects)
- the effect of not implementing the Change
- the IT, business, administrative and other resources required to implement the Change, covering the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required
- the current schedule of Changes
- additional, ongoing resources required if the Change is implemented.

Based upon these assessments, and the potential benefits of the Change, each of the assessors should indicate whether they support approval of the Change. CAB members should also decide whether they are content with the priority assigned by Change Management and be prepared to address any alterations they see as necessary.

CAB members should come to meetings prepared to make decisions on which Changes should go ahead, based on the priority assessment of the Changes. The CAB should be informed of any Changes that have been implemented as a work-around to Incidents and should be given the opportunity to recommend follow-up action to these.

Note that the CAB is an advisory body only. If the CAB cannot agree to a recommendation, the final decision on whether to authorize Changes, and commit to the expense in resources involved, is the responsibility of the Change Manager. Depending on the nature of the Change, references to Service Level Agreements may be required. In some cases, Customer sign-off will be required at some point.

When emergency problems arise, there may not be time to convene the full CAB, and it is therefore necessary to identify a smaller organization with authority to make emergency decisions. Such a body is known as the CAB Emergency Committee (CAB/EC). The composition of the CAB needs to be flexible, in order to represent business interests properly when emergency Changes are proposed. It will also ensure that the composition of the CAB/EC will provide the ability, both from a business perspective and from a technical standpoint, to make appropriate decisions in any conceivable eventuality.

### **6.3 Change Governance Board**

The Change Governance Board (CGB) is a body that exists to provide guidance and senior management acceptance of large scale, high-impact change requests. Requests that will affect the major University mission, re-align major services, etc. should be escalated to this body to ensure clear definition and buy-in is given. Likewise, this body serves as an escalation point for those instances when a change cannot be agreed upon or an acceptable schedule developed. While expected to be very rare, the Change Manager can convene this body to review issues not resolvable at the CAB level.

The CGB membership should be comprised of:

- The Change Manager
- The Vice-President of Information Technology
- Divisional Executive Directors
- Security Officer
- Communications Officer
- Technology Officer

The primary duties of the CGB members are:

- Review RFC's escalated to the group
- As appropriate, be available for consultation on urgent changes
- Provide decisions on the viability of major changes, impacts on operations and service and provide guidance to the Change Manager in order to reach a decision

Upon scheduling a CGB session the Change Manager will provide all members with the RFC, supporting documentation, FSC, and overview of issues pertaining to the change and why it is in question. The Change Initiator and Change Owner will attend this session to resolve questions or issues as any may arise.

Upon review by the CGB and assessment of the change a decision to approve or disapprove will be reached and documented by the Change Manager and addressed accordingly.

## **6.4 Divisional Change Coordinator**

The Divisional Change Coordinators (DCC) are appointed by the Divisional Executive Director to preside over the Divisional Change Management Program. Operating in an identical environment as that of the CCIT Change Manager, the DCC chairs the Divisional CAB and manages all changes requested at the Division level. Responsibilities of the DCC include:

- Receive, log and allocate a priority, in collaboration with the initiator, to all RFCs within their respective division. Reject any RFC that is impractical.
- Present all RFCs at a Divisional CAB meeting, issue an agenda and circulate all RFCs to Divisional CAB members in advance of meetings to allow prior consideration.
- Liaise with all necessary parties to coordinate Change building, testing and implementation, in accordance with schedules.
- Update the divisional Change log with all progress that occurs, including any actions to correct problems and/or to take opportunities to improve service quality.
- Review all implemented divisional Changes to ensure that they have met their objectives. Refer back any that have been backed out or have failed.
- Review all outstanding divisional RFCs awaiting consideration or awaiting action.

- Analyze Divisional Change records to determine any trends or apparent problems that occur. Seek resolution with relevant parties.
- Produce regular and accurate management reports.
- Escalate changes affecting any production service or impacting customers to CCIT Change Management as appropriate
- Represent divisional interests as a member of the CCIT CAB, CAB/EC, and CGB as appropriate.

## **6.4 Divisional Change Advisory Boards**

Each Division within CCIT will institute a Divisional Change Advisory Board with the intent of providing the same type of review and oversight for all divisional changes in the same manner as that of the CCIT Change Advisory Board.

The Divisional CABs should consist of the individual unit managers within each Division. This group, with guidance provided by the Divisional Change Coordinator schedules and manages RFC's within the division. Those RFCs affecting CCIT's production systems and services, upon approval by the Divisional CAB must be escalated and to the CCIT Change Management program for review, approval, communication and scheduling

The level of formality of this body is left to the discretion of the Executive Director for each Division within CCIT. Formalized bodies within each Division may not be necessary. Change scheduling and review may be conducted in Manager meetings or planning sessions, rather than large-scale, formalized Change Management sessions. It is important to note at this point, however, regardless of the formalization of Divisional Change Management all changes impacting services to customers must be escalated to the formal CCIT Change Management program.

## **6.4 Change Initiator**

The Change Initiator is the staff member submitting the Request for Change (RFC). Any staff member within CCIT may submit a Request for Change. The Change Initiator will work with the Divisional Change Coordinator and, as appropriate the Change Manager to ensure that the RFC is complete and accurate.

## **6.5 Change Owner**

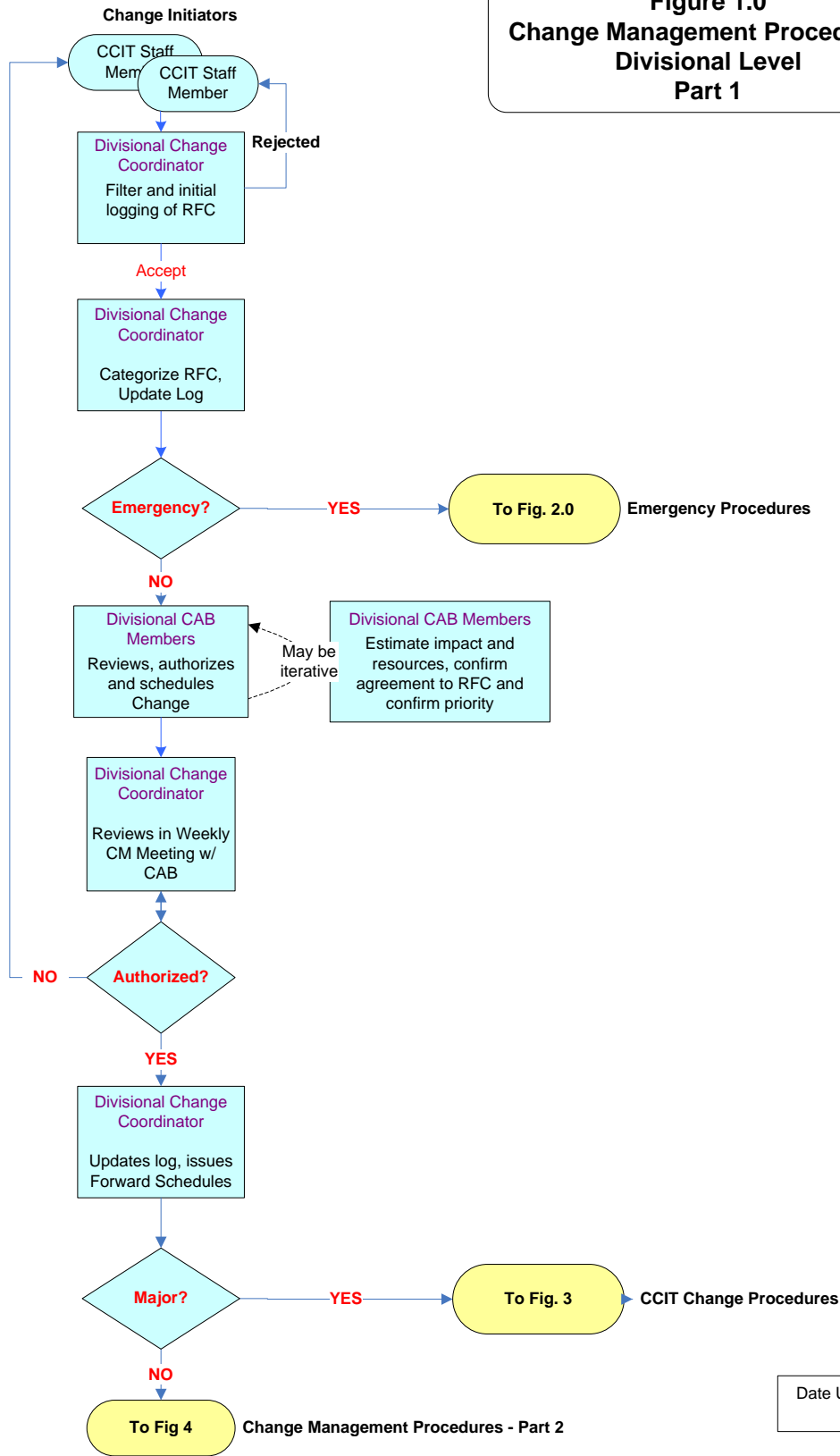
The Change Owner is identified in the Request for Change (RFC) form and is responsible for seeing to the planning and implementation of the proposed Change. The Change Owner may be a developer, subject matter expert or the CI's supervisor. The Change Owner is also responsible for communicating the Change to the appropriate parties, such as the CCIT Communications group and the customer and keeping the Change Manager informed throughout release cycles.

## **7.0 The Change Management Process – 8 Steps**

All members of the CCIT organization are authorized to request changes. Otherwise, innovation might be stifled or important concerns may go unreported. All Changes should be approved by the staff member's, otherwise known as the Change Initiator, manager/supervisor, otherwise referred to as the Change Owner prior to submission. This will filter out those requests that do not have the support of the

wider User community, or are impractical, and help collate similar or identical requests, thus reducing request volumes. Figures 1, 2 3 and 4 represent a flowchart of CCIT's Change Management process.

**Figure 1.0  
Change Management Procedures -  
Divisional Level  
Part 1**



Date Updated:5/15/07  
CM1.vsd

## 7.1 Logging

All RFCs received will be logged and allocated an identification number (in chronological sequence). The Change Manager will make sure all actions are recorded, as they are carried out, within the Change Management log. If this is not possible for any reason, then they should be manually recorded for inclusion at the next possible opportunity. Only the Change Manager is allowed to close an RFC. Details to be included in the RFC are:

- Requestor or Initiator
- Date submitted
- A clear description of the change requested, detailing systems involved and staff who will be required to implement
- The reason for the change - is it an enhancement, a new implementation etc? How will the University benefit from this implementation (if that is appropriate)?
- Evidence that thought has been put into a back out plan is also important. If the implementation of this change fails, you will need to back out to ensure normal University operations are not affected.
- The date you request to implement the change
- The date by which this change *must* be implemented (if other things are dependent on it for instance)
- Anticipated impact
- Priority
- Status
- Comments

## 7.2 Filtering

As Changes are logged, the Change Manager will consider each request and filter out any that are totally impractical or incomplete. These will be returned to the Initiator, together with brief details of the reason for the rejection, and the log should record this fact. A right of appeal against rejection exists, via normal management channels.

The Change Manager will notify the Initiator of acceptance or rejection and update the Change Management log.

## 7.3 Categorization

Categorization of RFC's is the weighing of the impact on our customers against the priority for the implementation of a change. Change Management must review each change to determine that the impact on our users is taken into account for each change, yet have the flexibility to implement changes in a short timeframe if the change is important. This "weighting" is conducted through the determination of 3 primary factors; Number of Customers Affected, the Duration of the Outage and the Priority need.

The Change Manager will categorize the RFC on several different scales to assess impact and urgency. Operational (routine, day-to-day) changes will proceed to Authorization and Scheduling. Major changes will be referred to the Change Advisory Board. Emergency changes may require that the Change Manager convene the Emergency Change Advisory Board (CAB/EC) as quickly as possible.

The Change Manager will assess the change according to:

**Impact:** How many customers will be affected by this change?

**Priority:** On what basis is the change being requested; e.g. self-generated, government mandated, security issue, etc.?

**Outage Durations:** Will any production systems be unavailable to customers?

**Systems:** Which IT Systems does this change affect?

Each of the aforementioned selections; Impact, Outage Duration and Priority are “weighted” to provide a value to the Change Manager. It’s important to note that the weight value of the Priority of a change is based on a “negative” number. Once the duration and the impact are measured, the Priority is subtracted from that total. So, the higher the Priority of the change, the shorter the time period required to implement. In this manner, large changes with large impacts can still be implemented very quickly should the priority of the change be a security-related issue such as a firewall problem.

Based on these values, the Change Manager and the Change Advisory Board utilize a scale to balance the scope of the change against the urgency of the change. The resulting comparison will provide baseline guidance to staff members to be used in planning for change implementations. Once the levels have been identified, the resultant sum will be balanced against a table of communications requirements. This table identifies the amount of time needed for communicating changes to the University. In short, the larger the categorization weighting the longer the amount of lead time required to implement a change.

The weightings are broken down as follows...

<b>Points Assigned</b>	<b>System Interruption Duration</b>
1	Level 1 – 0 -1 Minute
2	Level 2 – 2 – 15 Minutes
3	Level 3 – 16 – 30 Minutes
4	Level 4 – -31 – 60 Minutes
5	Level 5 – 61 – 120 Minutes
6	Level 6 –121 – 180 Minutes
7	Level 7 – 180 – 240 Minutes
8	Level 8 – 4 – 6 Hours
9	Level 9 – More than 6 hours

<b>Points Assigned</b>	<b>Number of Customers Impacted</b>
1	Level 1 – 0 Customers Impacted
2	Level 2 – 1 – 100 Customers Impacted

3	Level 3 – 101 – 500 Customers Impacted
4	Level 4 – 501 – 1,000 Customers Impacted
5	Level 5 – 1,001 – 5,000 Customers Impacted
6	Level 6 – 5,000 or more Customers Impacted

Points	Priority Level
(-2)	Level I – Self-Generated/Not Urgent
(-4)	Level II – Minor User Functionality/Required
(-6)	Level III – Service Availability/Major Functionality
(-8)	Level IV – University/Government Mandated
(-10)	Level V – Security Issue

To determine the categorization of each change a formula is utilized;

**Outage Duration + Customer Impact + Priority Level = RFC Implementation Lead Time**

Categorization levels are defined as...

Categorization Total	Communication Time Required
0 – 3 points	8 Days
4 – 8 points	15 Days
9 – 12 points	22 Days
12 + points	30 or More Days

As an example, a change request that will require a 40 minute outage and impact 600 people to install a new, minor functional tool in the Course Management System (Blackboard) would require at least 15 days to conduct communications and coordination. The equation for this scenario would be...

**4 points      Level IV – 40 Minute Outage**  
**4 points      Level IV – 600 Customers Impacted**  
+      (-4) points      Level II - Minor User Functionality

**Categorization Level of 4 results in a 15 Day Notice & Preplanning**

Of course, if, within that 15-day period finals are being conducted or it is Christmas break, the scheduling can be adjusted shorter or longer, as determined by the Change Manager. This adjustment is within the authority of the CCIT Change Manager.

These categorizations will help to determine the level of authorization required (Scale) and contribute to the impact assessment, resource requirements and scheduling of the RFC.

Every RFC will be allocated a categorization based on the impact of the Problem and the urgency for the remedy. This priority rating is used to decide which Changes should be discussed and assessed first by the CAB. The Change Manager is responsible for assigning this categorization. The priority of RFCs ideally should be decided in collaboration with the Initiator and, if necessary, with the CAB; but it should not be left to the Initiator alone, as a higher priority than is really justified may result. **Risk assessment is of crucial importance at this stage.** The CAB will need information on business consequences in order to assess effectively the risk of implementing or denying the change.

Predefined change types are set out below. It is expected that the majority of RFCs will fall into the Operational and Major categories.

- **Emergency Change**

Causing loss of service or severe usability problems to a larger number of Users, a mission-critical system, or some equally serious problem where immediate action is required. Depending on the urgency of the Change to be made, the CCIT Change Manager will decide whether to talk to members of the CAB or to convene a CAB/EC. Prior to any meeting, all documentation should be circulated for impact and resource assessment. Resources may need to be allocated immediately to build such authorized Changes.

If a Change, once implemented, fails to rectify the urgent outstanding Problem, there may need to be iterative attempts at fixes. The Change Manager should take responsibility at this point to ensure that business needs remain the primary concern. It is important that each iteration is controlled in the manner described in this section. The Change Manager should ensure abortive Changes are swiftly backed out.

If too many attempts at an urgent Change are aborted, there are three questions that require addressing:

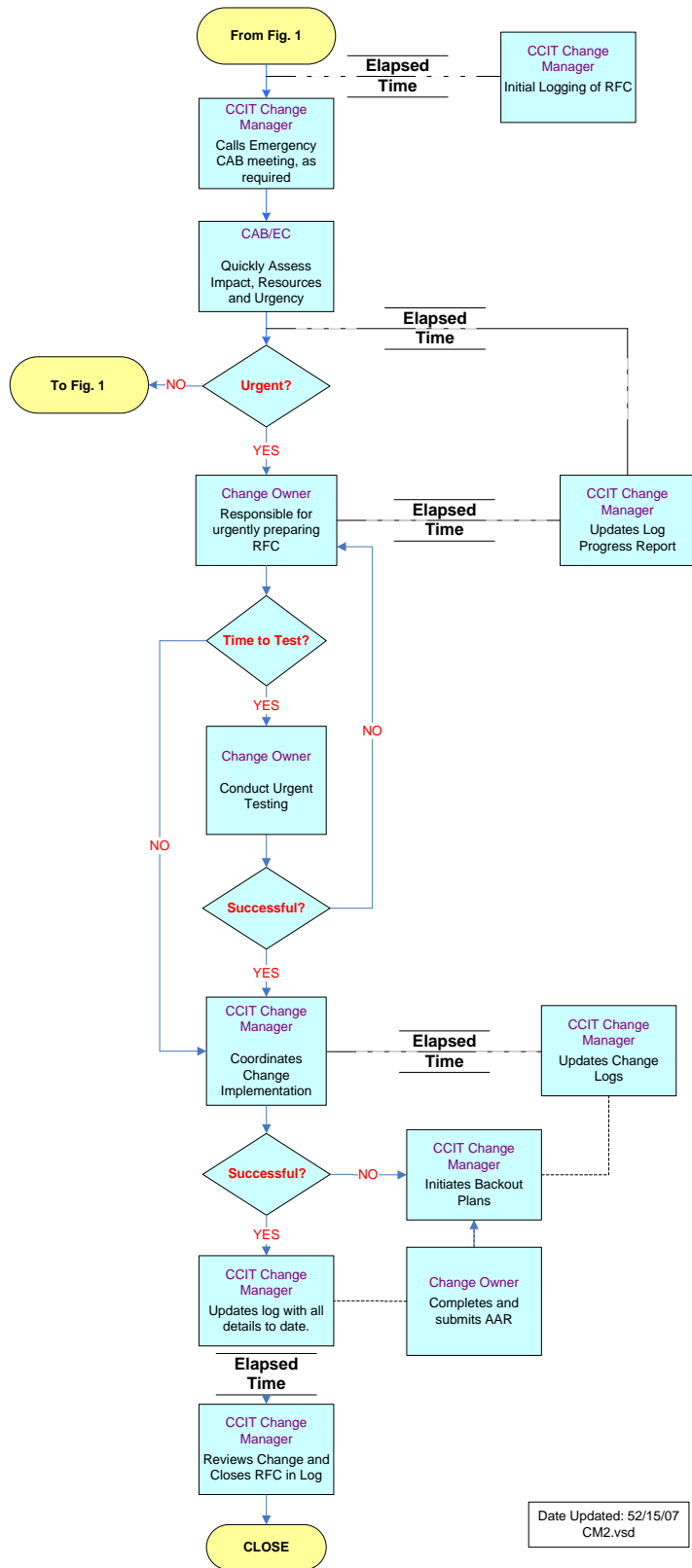
1. Has the Problem been correctly analyzed?
2. Has the proposed remedy been adequately tested?
3. Has the solution been correctly implemented?

In such circumstances, it may be better to provide a partial service, with some User facilities withdrawn, in order to allow the Change to be thoroughly tested, to suspend the service temporarily and then implement the Change.

It may not be possible to update all Change Management records at the time emergency actions are being completed (e.g. during overnight or weekend working). It is, however, essential that manual records are made during such periods, and it is the responsibility of Change Manager to ensure that all records are completed retroactively, at the earliest possible opportunity.

This is vital to ensure valuable management information is not lost. An example could be the updating of an attribute defining 'success', 'failure' or perhaps 'partial failure' of a Change.

**Figure 2.0  
CCIT Change Management  
Emergency Procedures**



Date Updated: 52/15/07  
CM2.vsd

## ▪ **Major Change**

The crucial elements to a Major Change are:

- the change will affect production environments
- tasks may not be well-known or may incur some level of risk
- authority may be given in advance, but proper scheduling and communication is required

Significant impact, and/or significant build or runtime resources required, or impact likely upon other parts of the organization. Severely affecting some Users, or impacting a large number of Users. To be given highest priority for Change building, testing and implementation resources. Rectification cannot be deferred until the next scheduled Release or upgrade. The Change Manager seeks advice from the CAB before proceeding.

## ▪ **Operational Change**

The key elements of an Operational Change are that:

- the change will **not** affect the production environments
- the tasks are well-known and proven or incur minimal risk
- authority is effectively given in advance
- budgetary approval will typically be preordained or within the control of the Change requester.

An Operational Change is justified and necessary, but can wait until the next scheduled release or upgrade. It has minor impact only, and few 'build' or additional 'runtime' resources are required. The Change Manager has the delegated authority to authorize and schedule such Changes, but these should be logged so that:

- records and work patterns can be identified
- accurate and complete costs for each service, Customer area etc, are available
- repetitive Changes, follow-on Changes, and associated Problem/Incident areas can be identified.

Recording every Change in summary helps to deliver an effective and efficient service to the Customer by allowing wastefully repetitive tasks to be spotted and eliminated. If the Change Manager has any doubts about authorizing any such Change, the Change can be referred informally to members of the CAB for a wider assessment.

## **7.4 Assessment**

Depending on the scale of the change as decided above, the RFC will be circulated either to the CAB members, or to a wider and more representative group.

The selected CAB members then assess the impact of this change in several different areas. Impact is measured on a scale of -5 (negative impact) to +5 (positive impact), allowing them to specify that the change is a good idea and will improve services, as well as to highlight areas of concern.

The initial assessment criteria which will be used are:

- Impact on business operations

- Impact on other operational systems
- Length of outage
- Number of users of the system impacted
- Impact on downstream systems
- Staff time required
- Impact on support staff
- Training requirements

The assessor will also be able to submit a written comment if they wish to highlight any concerns.

Assessments will be made electronically, however if there is no consensus on whether a change should proceed, a CAB meeting will be called. The change initiator may also be requested to attend the CAB meeting, if more information is required.

Assuming the CAB agrees upon their assessment, it will proceed to the next step, or be returned to the Initiator with an explanation of the areas they need to improve.

An electronic copy of all assessments will be maintained.

## **7.5 Authorization**

The change Manager can:

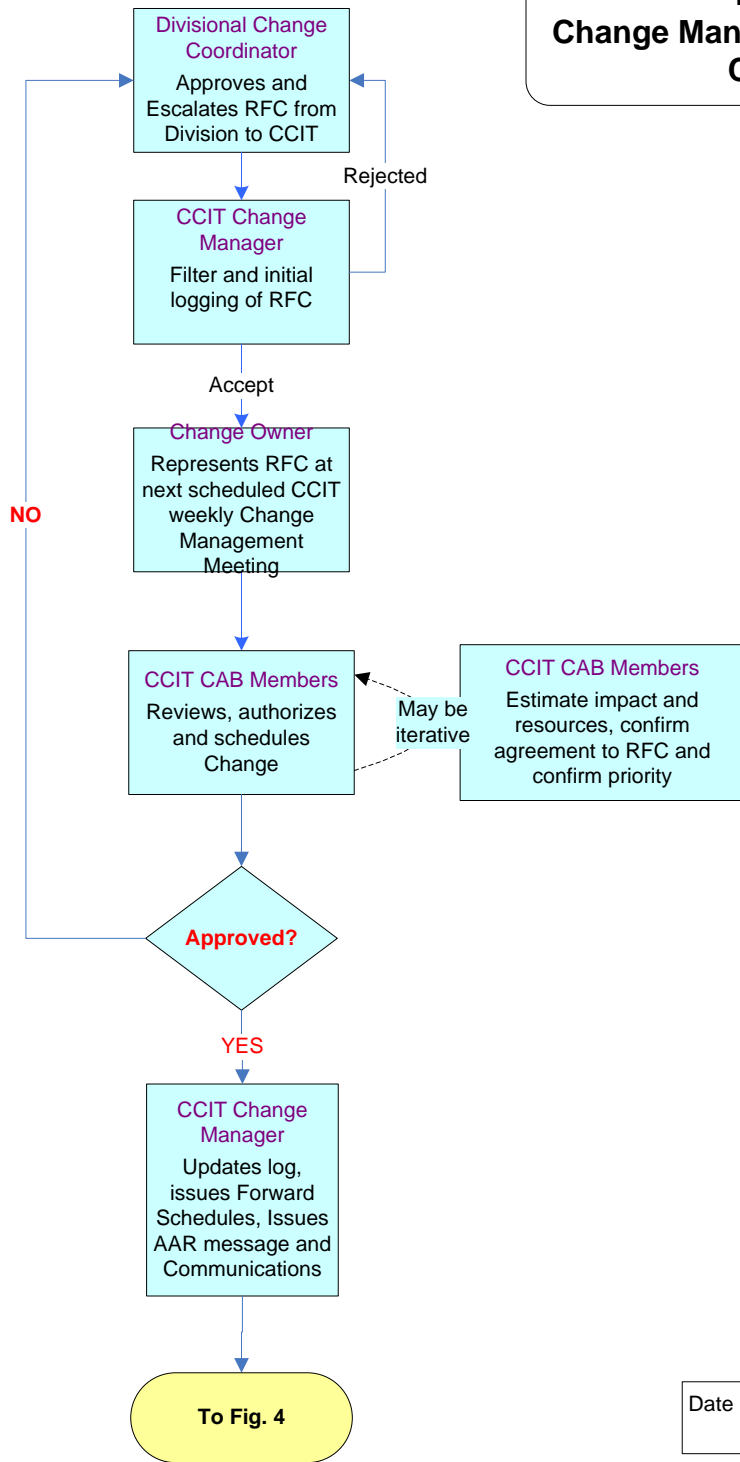
- Approve the change
- Refer the change to the CAB
- Reschedule the change to adhere to the Critical Dates Calendar
- Refer the change to a higher authority (executive sponsorship)

Depending on the scale of the change, it will be referred to the Initiator's immediate supervisor, or to a higher body if required. Many changes will be pre-approved, and this step will be redundant but necessary to ensure proper and complete communications.

## **7.6 Scheduling**

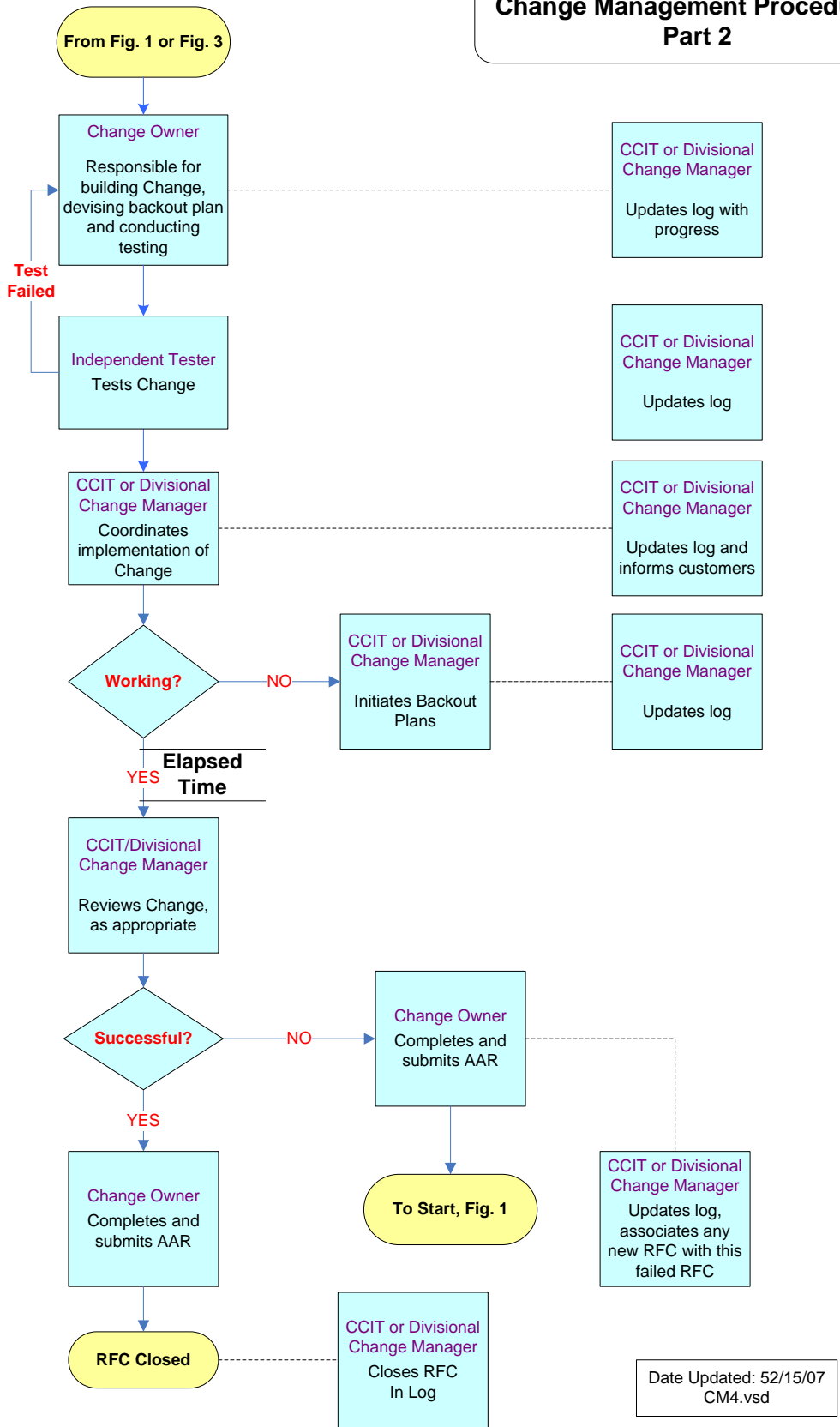
The Change Manager also maintains the Forward Schedule of Changes (FSC). If the date requested by the initiator of a change clashes with previously approved changes, a new implementation date may be requested, or other changes rescheduled (providing the current change has a higher priority). In all cases, the CAB will endeavor to work within the critical time constraints indicated on the Request.

**Figure 3.0  
Change Management Procedures -  
CCIT Level**



Date Updated: 5/15/2007  
CM3.vsd

**Figure 4.0**  
**Change Management Procedures -**  
**Part 2**



Date Updated: 52/15/07  
 CM4.vsd

## 7.7 Implementation

Authorized RFCs should be passed to the relevant technical groups for building the Changes. This might involve:

- building a new production module
- creating a new version of one or more software modules
- purchasing equipment or services externally
- preparing a hardware modification
- producing new or amended documentation
- preparing amendments to User training
- coordinate activities with appropriate communications units where pending changes need to be announced
- providing training to support staff

Building the change, testing the change, preparing roll-out plans, back out plans and actually performing the implementation will be the responsibility of the Change Owner. Progress will be tracked and communicated to the Change Manager.

## 7.8 Review

Following the successful implementation of a change (or otherwise), the Change Manager must review all implemented Changes after a predefined period has elapsed. This process may still involve CAB members; the Change Manager may look to them for assistance in the review process.

The purpose of such reviews is to establish that:

- the Change has had the desired effect and met its objectives
- Users and Customers are content with the results, or to identify any shortcomings
- there have been no unexpected or undesirable side-effects to functionality, availability, capacity/performance, security, maintainability etc.
- the resources used to implement the Change were as planned
- the implementation plan worked correctly (to include comments from the implementers)
- the Change was implemented on time and to cost
- the backout-plan functioned correctly, if needed.

Any problems and discrepancies should be fed back to CAB members (where they have been consulted or where a committee was convened), impact assessors, product authorities and Release authorities, so as to improve the estimating processes for the future.

Where a Change has not achieved its objectives, the Change Manager (or the CAB) should decide what follow-up action is required, which could involve raising a revised RFC. If the review is satisfactory or the original Change is abandoned, the RFC should be formally closed in the logging system.

Review will not need to be performed on every change successfully implemented, however it is a useful exercise to identify strengths about one implementation that can be successfully applied to others. For those changes where implementation was not successful, we need to ensure that we can learn from what went wrong, and identify ways to avoid the same pitfalls in the future.

These reviews will take place in the CAB meeting. The Change Manager will be responsible for closing and archiving the RFC.

## **7.9 Change Management Meetings**

Change Management meetings will be held on a weekly basis to review outstanding change requests. Minimally, the Change Advisory Board (CAB) should attend this meeting, as well as the Change Initiator (CI) or Change Owner (CO) for each Request for Change.

Chaired by the CCIT Change Manager, the purpose of this meeting is to review all requests, as represented by the CI or CO to the CAB. Additionally, the meeting is open to all CCIT Staff Members for informational purposes. By providing an overview of the change, its impact, duration and purpose all attendees will have the opportunity raise concerns or questions.

Approval or Disapproval of RFC's will lie with the Change Advisory Board, which must take into account any issues raised by attendees in the meeting. For those RFC's where a decision cannot be reached, the Change Manager holds final decision authority or may elect to escalate the RFC to the Change Governance Board, as defined in section 6.3.

Meetings will be held in as centrally located conference room as possible. All effort will be made to utilize technology to broadcast/simulcast/teleconference this meeting, as possible.

## **8.0 Reviewing the Change Management program for Efficiency and Effectiveness**

Change Management should initiate follow-up actions to correct any problems or inefficiencies arising in the Change Management program itself as a result of ineffective Changes. For example, a large Change backlog may indicate that Change Management is under-resourced; a high incidence of unsuccessful Changes indicates that Change assessment or Change building is not working satisfactorily. Change record reviews may also highlight problems in other processes, such as Problem Management, in the reliability of system components, or in staff's or users' procedures and/or training. These problems should be reported to the managers concerned and highlighted in the Change Management reports to management.

It is also recommended the Service Management Office review the Change Management process periodically for efficiency and effectiveness. Such a review should be carried out shortly after the Change Management process is implemented, to ensure that the plans were carried out correctly and that the process is functioning as intended. Any problems should be traced back to the source and corrected as soon as possible. Thereafter, regular formal reviews of the Change Management process should take place - at least every six months. The Change Manager should also continually assess the efficiency and effectiveness of the Change Management process.

It should be noted, with respect to any review, that a high number of RFCs does not necessarily indicate a problem with the Change Management process - it may just reflect volatile systems. Any attempt to reduce the number of RFCs may stifle innovation. The prime indicator of an effective Change Management process is that the right 'mix' of RFCs is maintained, not that the number of RFCs has been reduced over time.

Other indicators of an effective Change Management process include:

- a reduction of adverse impacts on service quality resulting from poor Change Management
- a reduction in the number of Incidents traced back to Changes implemented
- a decrease in the number of Changes backed out
- a low number of urgent (and therefore unplanned) Changes - this should include emergency, out-of-hours Changes referred back for clarification
- no evidence of Changes having been made without reference to the Change Management system
- close correlation between FSCs and the actual implementation of Changes
- no high-priority RFCs in backlogs, and the size of backlogs not increasing
- evidence of accurate resource estimating, when resource estimates are retrospectively compared with actual resources used
- regular reviewing of RFCs and implemented Changes, and the clearing of any review backlogs
- successful implementation of changes that clearly benefit the business and satisfy Customers
- a low incidence of unjustifiably rejected RFCs.

These items can be used as metrics for measuring the effectiveness and, to an extent, the efficiency of the Change Management process. In measuring that efficiency, it is necessary to consider, the amount of Change successfully implemented per unit of staff costs, including, for example, the costs of assessors, builders, and testers. This may be difficult to assess in absolute terms, but it should generally be possible to observe an increase in efficiency over time, especially in the early days of the Change Management process when the learning curve is steepest.

## **9.0 Benefits, Costs, and Possible Problems**

### **9.1 Benefits**

Efficient Service Management requires an ability to change things in an orderly way, without making errors or making wrong decisions. *Effective* Change Management is indispensable to the satisfactory provision of services, and requires an ability to absorb a high level of Change. Specific benefits of an *effective* Change Management system include:

- better alignment of IT services to business requirements
- increased visibility and communication of Changes to both business and service-support staff
- improved risk assessment
- a reduced adverse impact of Changes on the quality of services and on Service Level Agreements (SLAs)
- better assessment of the cost of proposed Changes before they are incurred
- fewer Changes that have to be backed-out, along with an increased ability to do this more easily when necessary
- improved Problem and Availability Management through the use of valuable management information relating to changes accumulated through the Change Management process
- increased productivity of Users - through less disruption and, higher-quality services
- increased productivity of key personnel through less need for diversion from planned duties to implement urgent Changes or back-out erroneous Changes
- greater ability to absorb a large volume of Changes
- an enhanced business perception of IT through an improved quality of service and a professional approach.

### **9.2 Costs**

The two principal costs of Change Management are for staff and software tools support.

- **Staff costs**

Staff costs include costs for the Change Management role and team, CAB members, and Change builders. These costs should be outweighed by the benefits that will be gained. In practice, most organizations already have a number of people who are spending time on handling Changes.

Although recommendations within this document may appear to increase the amount of management time spent on Changes, in practice management will spend less time on Changes as the need to handle issues arising from ineffective Change Management is eliminated.

- **Support tools**

The cost of support tools, together with any hardware requirements, needs to be considered. Although tools that integrate support for Change Management, Configuration Management, Problem Management and Service Desks are likely to be more expensive than 'simple' Change Management tools, the additional cost is often justifiable. For larger organizations, management processes can be virtually impossible to implement effectively without adequate support tools.

### **9.3 Possible problems**

The Change Management process should be appropriate to the size of the organization; an over-bureaucratic process can diminish effectiveness. Paper-based systems are difficult to administer and often result in bottlenecks.

There may be cultural difficulties in getting staff, Customers and Users, to accept that a single Change Management system should be used for all aspects of an infrastructure. It may require education to convince everyone that all components of an infrastructure can, and very often do, impact heavily upon each other, and that Changes to individual components require coordination. Attempts may be made to implement Changes without reference to the Change Management process. Measures should be introduced to prevent and detect such illicit changes, by conducting regular independent audits to check that Change Management staff, other Service Management staff and Users are adhering to the Change Management procedures.

Other potential problems that may arise are:

- the scope of a Change is too wide for the resources available, over-stretching the staff and causing delays
- ownership of the impacted systems is unclear, resulting in delays and incomplete assessments
- the process is too bureaucratic giving excuses for not following it
- inaccurate configuration data may result in poor impact assessments leading to the wrong people being consulted about the Change
- poor synchronization of upgrades between platforms and across locations makes Changes difficult or impossible to schedule
- back-out procedures are missing or untested
- progressing Change requests is manually intensive; it is advisable to start with a simple database or an automated system
- lack of backing from senior and middle managers will lengthen implementation times, staff will resist the controls that they would prefer to avoid unless they can see the commitment from management

- the process frequently fails when emergency Changes should be done.

## **Glossary**

### **Change**

The addition, modification or removal of approved, supported or baseline hardware, network, software, application, environment, system, desktop build or associated documentation in the production infrastructure.

### **Change Advisory Board**

An authoritative and representative group of people who are responsible for assessing, from both a business and technical viewpoint, all high impact RFCs. They advise the Change Manager on the priorities of RFCs and propose allocations of resources to implement those Changes. The CAB will be made up of Customer, User and IT representatives and may also include, depending upon the nature of the Changes being considered, 3<sup>rd</sup> party and other administrative business representatives. The CAB is chaired by the Change Manager.

### **Change Advisory Board / Emergency Committee**

An emergency meeting of the CAB, usually with a reduced number of members, to consider urgent, high impact Changes. Its membership, which may change from occasion to occasion, therefore needs to represent the knowledge and authority required in these exceptional circumstances. In practice, members may make their decisions without a physical meeting.

### **Change Initiator**

Initiates the RFC. Follows processes for submitting an RFC and provides input in the post-implementation review.

### **Change Log**

A log of Requests for Change showing information on each Change, its evaluation, what decisions have been made and its current status, e.g. Raised, Reviewed, Approved, Implemented, Closed.

### **Change Management (Change Manager)**

The Service Management process responsible for controlling and managing requests to effect changes (RFCs) to the IT Infrastructure or any aspect of IT services to promote business benefit while minimizing

the risk of disruption to services. Change Management also controls and manages the implementation of those changes that are subsequently given approval.

### **Change Owner**

A general term, signifying principal responsibility. A senior manager with overall responsibility for ensuring the stability of a process or service.

### **Emergency Change**

A Change planned, scheduled and implemented at very short notice in order to protect a service from an unacceptable risk of failure or degradation, lack or loss of functionality.

### **Forward Schedule of Changes**

A schedule that contains details of all Changes approved for implementation and their proposed implementation dates.

### **Impact**

A measure of the effect that an Incident, Problem or Change is having or might have on the business being provided with IT services.

### **Incident**

An event which is not part of the standard operation of a service and which causes or may cause disruption to or reduction in the quality of services and Customer productivity.

An Incident might give rise to the identification and investigation of a Problem, but never becomes a Problem.

### **Major Change**

A Change that will have significant impact, and/or significant build or runtime resources required, or impact likely upon other parts of the organization. Severely affecting some Users, or impacting upon a large number of Users. To be given highest priority for Change building, testing and implementation resources. Rectification cannot be deferred until the next scheduled Release or upgrade. The Change Manager seeks advice from the CAB before proceeding.

## **Operational Change**

An Operational Change is justified and necessary, but can wait until the next scheduled release or upgrade. It has minor impact only, and few 'build' or additional 'runtime' resources are required. The Change Manager has the delegated authority to authorize and schedule such Changes.

The crucial elements of an Operational Change are that:

- the tasks are well-known and proven
- authority is effectively given in advance
- the train of events can usually be initiated by the Service Desk
- budgetary approval will typically be preordained or within the control of the Change requester.

## **Problem**

The unknown root cause of one or more existing or potential Incidents. Problems may sometimes be identified because of multiple Incidents that exhibit common symptoms. Problems can also be identified from a single significant Incident, indicative of a single error, for which the cause is unknown. Occasionally Problems will be identified well before any related Incidents occur.

## **Request for Change**

A means of proposing a Change to any component of an IT Infrastructure or any aspect of an IT service. It may be a document or record in which the nature and details of, and the justification and authorization for the proposed Change are entered.

## **Request for Service**

A request for a change, usually both common and straightforward, to be made to a service. A RFS is characterized by the fact that the Change can be made under strict, well-defined procedural control and is therefore (virtually) risk-free.

## **Urgent (or Emergency) Change**

A change that must be introduced as soon as possible to alleviate or avoid detrimental impact on the business.