Infrastructure
Change Management

The process and procedures for all changes to the live environment

Version 4.1 October 2012
1.0 Introduction ........................................................................................................... 3
2.0 The Change Process ................................................................................................. 4
  2.1 Why raise a change? .......................................................................................... 4
  2.2 Who can request a change? ............................................................................... 4
  2.3 When to raise a change depending on change type? ........................................... 4
  2.4 How to raise a change ....................................................................................... 5
  2.5 What is a request for change? .......................................................................... 5
  2.6 Change terminology ......................................................................................... 5
  2.7 Change management process ........................................................................... 5
  2.8 Change approval board .................................................................................... 5
  2.9 Change communication .................................................................................... 5
  2.10 Completed changes ......................................................................................... 6
  2.11 Post implementation review ........................................................................... 6
3.0 Completing a Request for Change ........................................................................... 6
  3.1 RFC Title/Project Code/Raised By/Authorised By ............................................. 6
  3.2 Proposed date/time/duration/location ................................................................ 6
  3.3 Description of change ....................................................................................... 7
  3.4 Impact of change .............................................................................................. 7
  3.5 Risk and issues analysis ................................................................................... 9
  3.6 Back-out plan ................................................................................................ 9
  3.7 Test plan ......................................................................................................... 9
  3.8 Potential business impact ............................................................................... 10
  3.9 Other systems/services impacted ..................................................................... 10
  3.10 Impact on disaster recovery ......................................................................... 10
  3.11 Planned resource .......................................................................................... 10
  3.12 Additional comments ................................................................................... 10
4.0 Submitting a Late Request for Change .................................................................... 11
5.0 Submitting an Emergency Request for Change ..................................................... 11
  5.1 Background ................................................................................................... 11
  5.2 Process .......................................................................................................... 11
6.0 The Generic Request Process ................................................................................... 12
  6.1 Background ................................................................................................... 12
  6.2 Process .......................................................................................................... 12
7.0 The Failed Change Process ..................................................................................... 13
8.0 The Change Process Review ................................................................................... 13
9.0 APPENDIX A: Data changes and SITS hotfixes .................................................... 14
10.0 APPENDIX B: Risk Issues Template ................................................................... 15
11.0 APPENDIX C: Version of Process Document ...................................................... 16
1.0 Introduction

The purpose of this document is to inform users of the infrastructure change management process and the procedure to follow when creating a request for change (RFC).

Change management is the practice of ensuring that all changes to configuration items are carried out in a planned and authorised manner. This includes ensuring that there is a business reason behind each change, identifying the configuration items and IT services affected by the change, planning the change, testing the change and having a back out plan should the change result in an unexpected state of the configuration item.

It is generally accepted that change management and configuration management are best planned and implemented concurrently, as this enables the organisation to weigh the risks and consequences of not implementing either process properly at the planning stages.

Change management is responsible for managing change processes involving:-
- Hardware/firmware
- Communications equipment and software
- Systems software
- ‘Live’ applications software
- All documentation and procedures associated with the running, support and maintenance of live systems.
- Personal computing standards

As no specific change management application software is currently available the system has been set up with the tools to hand viz: e-mail (for request submissions) and MS Office applications (Excel/Word for management and consistency of submission).

The Infrastructure Team Quality Manager is responsible for the collation of the RFCs, preliminary Quality checks and the distribution of request ‘packs’ to Change Advisory Board (CAB) members in a timely fashion, the secretarial responsibilities of the Board and the upkeep and dissemination of the change calendar, post meetings.

The CAB is composed of senior representatives (Senior Infrastructure Engineers, Senior Systems Architect and Senior Support Analyst) from the IT Services Teams, chaired by the Director or an Assistant Director (AD), (based on the Duty Manager rota), but may be complemented, on an ad-hoc basis, by invited guest attendees in order to (1) spread the culture and understanding of the process, and, (2) to provide additional expertise and advice.

The CAB provides a forum for the discussion of proposed changes, their impact, any conflict resolution and their scheduling.

In some cases, if a change is affecting a specific user or if an upgrade is required for a vendor supplied application then the change may be referred the Director of IT Services.

It is proposed that the CAB meet weekly and the changes submitted in a scheduled and timely manner in order to allow the CAB members to review the proposals prior to the meeting, and to enable additional attendees to be co-opted as required.
RFCs must be approved by the CAB. It is assumed that RFC Raisers have user signoff prior to raising RFC for CAB and remain responsible for user acceptance.

2.0 The Change Process

This section is designed to explain the rationale behind the change control process – Why, Who, When, How and What. (Note: There is a slightly different process for changes relating to SITS, which can be found at Appendix A). The change Process should be reviewed every 6 months.

2.1 Why raise a change?

There are a number and variety of systems in the University campus areas. Any changes to the LIVE system platforms, networks or applications must be registered and approved as such in order to protect the user base and yourself (the instigator of the change).

2.2 Who can request a change?

Anyone within IT Services Service Area can request a change; however, it must be agreed by their line /project manager before being forwarded to the change manager. This is a first filter to ensure only relevant and necessary RFCs are seen by the CAB. It is recommended that a senior technician also reviews the content of an RFC as a peer review.

2.3 When to raise a change depending on change type?

Notification of a change depends upon the impact to others – the greater the notice period the greater the chance of securing an implementation date in the change calendar. There are four categories of change:

- **Normal**
  to arrive with change manager by Friday preceding CAB on the Wednesday giving a minimum 5 working days notice prior to intended implementation. Approval by a senior management team member is required.

- **Late**
  arrives later than Friday but is not an Emergency. less than 5 working days notice will require approval from a CAB member.

- **Emergency**
  this would normally occur in response to a problem and would require implementation immediately to resolve or prevent a LIVE service outage; this would require approval from an Assistant Director/Director of IT Services.

- **Generic**
  used to accommodate repetitive task with little or no effect on, or risk to, the production environment.

- **Data**
  Used for low complexity low impact changes to reports or data. Incorporates Hotfixes to SITS . These receive a light touch at CAB and are submitted for information only. Approval by a lead technician is sufficient.
2.4 How to raise a change

A change should be raised by e-mailing the proposal (using Request for Change Template) to the Change Manager at changemanager@anglia.ac.uk.

2.5 What is a request for change?

An RFC supports an action that is one or all of the following:

- Affects more than one person.
- Causes a system outage by an alteration/restart to any existing system.
- Involves a new release of an application/component/platform.
- Upgrades an application/component/platform.

2.6 Change terminology

Any change that meets the above criteria is known as a strategic change. Other requests (such as password reset; directory access or additional software request) will be treated as problem requests and should be handled as such by raising a SupportWorks call with the Customer Support Team.

2.7 Change management process

Once a change has been raised it will undergo a stringent process of evaluation to include: business need, date availability, clashes, impact, risk assessment, approval and post change review. Induction and refresher training is available on request from the Change Manager.

2.8 Change approval board

The CAB meets weekly every Wednesday to provide a forum for discussion on forthcoming changes, their impact, scheduling and any areas of potential conflict. Permanent CAB members are the IT Services Director, Assistant directors, BRMs and all Senior IT Services Staff. Not all of these will be in attendance each week however.

CAB does not have a quorum but requires chairing by a senior management team member (usually the Dutymanager for that week) and a Customer Support Team representative (plus a rep for each RFC submitted to ensure its approval).

In the event that a change will have a high impact on a critical system or a software/operating software upgrade is required to a vendor supplied application or platform, then the change should be referred to the Director of IT Services.

2.9 Change communication

All logged changes will be shown on a change log providing forthcoming change activity for the future month ahead. Communication of the change to users is dependent on the type and extent of the change. Communication of changes to users should be looked at on a case by case basis, in conjunction with Senior Support Analysts and Business Relationship Managers. All communications should
pass via the Communications team headed up by the CST Assistant Director and my.anglia notices posted by a CST senior analyst.

2.10 Completed changes

Once a change has taken place the person who requested the change will contact the Change Manager to confirm whether or not it was successful, as well as offering details of any lessons learnt or areas to flag for possible further change.

2.11 Post implementation review

Once the change has been completed, a post implementation review may take place, depending on the success and nature of change. The purpose of such review will be to establish that the:

- change has had the desired effect and meets its objectives
- users and customers are content with the result
- resource used to implement the change were as planned
- implementation plan worked correctly
- back-out plan functioned effectively (if needed); and that
- no unexpected side-effects occurred

3.0 Completing a Request for Change

3.1 RFC Title/ Project Code/ Raised By/ Authorised By

- RFC Title should be brief description of change ,
- Project code is the IT Services Project Number allocated or SupportWorks which initiated the Change
- Raiser is the person responsible for attending CAB or sending delegate
- Authoriser is responsible for ensuring validity of content and that all testing is complete prior to go-live

3.2 Proposed date/ time/ duration/ location

- Changes will need to be completed and submitted by close of play Friday in order to be collated and reviewed by the CAB on the following Wednesday.
- Changes received after the Friday preceding the RFC’s final CAB (ie. The final CAB meeting preceding its implementation date) will be considered Late changes
- The CAB will receive copies of the RFCs by close of play Monday.
- Note that the request should include the proposed start and end date and times for the change. Consideration must be given here for the implementation of any back-out plan, should it be necessary.
3.3 Description of change

The description should:

- State the area and reason for change i.e. user request, enhancement, business requirement, service call/incident/problem, fixes
- Explain to the layman what the change is, and why it should be carried out, specifically detailing all systems/services that will be affected.
- Explain (if appropriate) why the change is business critical (this is particularly important at specific times of the academic year) or what its impact is on the business.
- Include a technical description of the change (this should include the steps which are to be performed in order to complete the change) and list the hardware components involved.
- Detail what testing has been carried out to date (why are we confident that the change is necessary?) and who was responsible for this. Also detail post-implementation testing activities.
- Indicate which users are affected and whether they have been made aware of the change.
- Indicate whether the change is a part of a bigger change or project.

3.4 Impact of change

This will be assigned on a scale of 1-5, where 1 is low, and 5 is high. The following table outlines the definition of the levels of impact.
<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Definition</th>
<th>Test &amp; Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>High potential impact to large number of users or business critical service. This change is global in its nature (University wide). System downtime is required. Example:- Introduction of new product, software, topology or feature.</td>
<td>Requires significant validation of new solution (potentially involving Architecture &amp; Development) including documented testing, validation and ‘what-if’ analysis showing impact to existing infrastructure; completion of support documentation, back-out plan, risk assessment and implementation plan. It is recommended that the solution is first piloted and a design review is carried out before testing.</td>
</tr>
<tr>
<td>4</td>
<td>High potential impact to large number of users or business critical service. Change probably requires system downtime. Example:- Large increase in traffic or users, backbone or network routing changes.</td>
<td>Requires ‘what-if’ analysis performed to determine the impact to the existing environment; testing, implementation, risk analysis and back-out plans. A design review for any major infrastructure changes.</td>
</tr>
<tr>
<td>3</td>
<td>Medium impact to smaller number of users or business service. Example:- As 1 &amp; 2, but fewer users affected.</td>
<td>Requires analysis of new solution which may require A&amp;D validation. Will require implementation, risk analysis and back-out plan.</td>
</tr>
<tr>
<td>2</td>
<td>Low potential impact. Example:- Adding new standard template modules, providing additional proven access services.</td>
<td>Requires implementation and back-out plan.</td>
</tr>
<tr>
<td>1</td>
<td>No user or service impact. Example:- adding individual users to network; standard configuration changes (password change, monitoring discovery or similar configuration parameters), no expected service or user downtime.</td>
<td>Low impact low complexity change eg. Data or report change</td>
</tr>
</tbody>
</table>
3.5 Risk and issues analysis

The amount of detail required in the risk analysis will be dependent upon the impact of the change. For all changes with an anticipated impact level of 3-5, a risk/issue log must be created.

A risk and issues template (Risk Issues Template) should be used in order to assist with the risk analysis assessment. On this template there is one tab for recording risks and another for recording issues. There is a comment in the title box of each column which should assist with the completion of the form.

3.6 Back-out plan

The amount of detail required in the back-out plan will be dependent upon the impact of the change. A back-out plan must be created for all changes with an anticipated impact level of 2-5 (see 3.3 above)

There are two elements to the back-out plan:-

1) How the change will be backed out if a problem is encountered whilst the change is being made.
2) How the change will be backed out if a problem subsequently occurs (post change) during business hours.

A list of personnel who should be available in the event of invocation of the back-out plan should be included.

A mandatory requirement is that the time at which the back-out plan should be invoked, if necessary, should be included in order to remain within the proposed time window.

The time required in order to execute the back-out plan should also be included. (i.e. the time required to restore the status quo).

The plan will include all personnel/third party contact details, as necessary, who will contact them, and under what circumstances.

3.7 Test plan

This should detail the testing either carried out prior to the change request being completed or planned prior to the change (if conditionally approved). A hyperlink to the test plan is advised. The amount of detail required will be dependent upon the impact of the proposed change.

Details required are:-

- What testing has already taken place, or is planned in order to ensure the maximum chance of success (pre-implementation test plan).
- What testing will take place after implementation to ensure that the change was successful (post-implementation test plan).

The following information should be provided:

- How was/is the change to be tested?
- How did/will the testing take place?
- Who will perform the tests?
- Does anyone need to be on standby during the tests?
• Who has agreed/signed off that the change is ready to be implemented?
• Who has agreed/signed off that the testing has been completed successfully?
• Who has agreed/signed off the test plan?
• Who will be notified that the change has/has not been completed successfully?

3.8 Potential business impact

If the change were to subsequently fail during business hours, which users would be affected, and for how long?
If the change were to fail during the change implementation, and had to be backed out, what would be the business impact of not carrying out the change?
If the change were to be rejected by the CAB what would be the business impact?
Consideration should be given to the timing of the change; business critical times should be avoided, if possible.

3.9 Other systems/services impacted

Any impact on other services or systems must be understood and explicitly stated in the request.

3.10 Impact on disaster recovery

If there is an impact on disaster recovery then this should be detailed in a separate document.
If the application/service is new - has a disaster recovery plan been created? Has this been agreed with the users?
If a major change is required has the impact on the existing disaster recovery plan been considered? Consultation recommended with Infrastructure AD as required.

3.11 Planned resource

Have the necessary resources (i.e. staff) required in order to successfully complete the change been agreed and are available?
It is the responsibility of the person raising the change to ensure that is properly resourced.

3.12 Additional comments

Any other relevant or additional information which may be of interest to the CAB should be included. This would include a completed Operational Acceptance Checklist for Project Implementations.
4.0 Submitting a Late Request for Change

A change that is submitted after the normal notification period will be deemed as a late RFC. These requests should be exceptional, and would normally be in response to an abnormal, or fault, situation. This may not be seen by the CAB to approve, therefore pre-approval must be sought from one of the CAB members.

Following the successful approval of the request, this should be confirmed to the Change Manager, with a copy of the change request and the approval, either by e-mail or a hard copy.

The CAB will review both the RFC and the reason for it being late, at the next meeting.

5.0 Submitting an Emergency Request for Change

5.1 Background

Much as it would be ideal to be able to plan for all changes, there are events that occur (production problems) that will require an emergency change. The purpose of this section is to outline the parameters and processes to accommodate such changes.

5.2 Process

Emergency changes must only relate to the resolution or prevention of production problems.

If the problem occurs during normal working hours the change must be approved by the Duty manager plus a senior management team member(either by phone/e-mail or face to face contact). This ensures a full understanding of the request and the rationale prior to approval.

If a change is required outside normal hours then pre-approval from the duty manager and an AD must be sought if:-

- The ‘impact level’ is 3-5
- It is believed that there is a likelihood that normal service will not be restored prior to the start of the next normal working day
- The individual is uncertain as to whether CAB authorisation is required.

The AD member who is contacted should preferably be the AD with expertise in the area of concern. In the event that the occurrence is out of normal hours then the permission of the Duty Manager must be sought (in addition to the AD if not the same person).

AD pre-approval is not required if the ‘impact level’ is 1-2 or is covered by a generic change request, and the change can proceed without further authorisation.

An RFC must be completed and emailed to the change manager post-action in order that the change and the problem can be tracked and accounted for. The CAB will review the RFC at the next meeting.
6.0 The Generic Request Process

6.1 Background

A generic request for change is designed to accommodate repetitive tasks that have little or no impact or risk on the production environment. The request will not differ in creation, only in detail and time of execution.

Examples are – installation of print drivers/refreshing a locked application/month end system processing.

It is important that these requests are logged in the change management system by raising a Normal RFC so that an audit trail exists, however, once the initial request has been approved, ‘generic’ subsequent submissions do not require CAB approval.

6.2 Process

Each initial generic request will be submitted to the Change Manager and will be presented to the CAB for approval. Once approval is granted, the change will be identified as the master change and assigned a unique identifier. The CAB will determine a time for review and re-approval for each master change.

To instigate a subsequent generic change, the requestor should e-mail the request to the Change Manager specifying the unique identifier or ‘base’ RFC number, the date, time and location of the changes and details of the implementers (if different to the requestor).

The Change Manager will manage and control these requests and on receipt will assign for implementing. They will not be presented to the CAB as they have been pre-approved.

The Change Manager will enter each change request into a spreadsheet or database which will contain a number of auditable features:

- description of each request with it’s unique number
- requestors name and details
- date of CAB approval
- date of CAB re-approval
- date of each invocation of the request.
7.0 The Failed Change Process

The purpose of the failed change report is to note the failure details of a change as soon after the event as possible, this will then assist in the identification of problems and assist in the future successful implementation of the change.

If the change is to be attempted again, another RFC should be submitted to the Change Manager, which refers to the original RFC, so that it can be tracked separately.

The completed report should be emailed to the change manager and distributed to the CAB for the next meeting.

8.0 The Change Process Review

The Change Process should be reviewed every 6 months as recommended by ITIL

This will occur in April and October each year

The meeting should be chaired by a director or assistant director of IT Services

Minutes can be found on the Infrastructure Change folder within Quality Management area.
9.0 APPENDIX A: Data changes and SITS hotfixes

The process for changes to Business Applications including SITS is different to the infrastructure change process, because of the nature, impact and frequency of changes that take place. The following is a general overview of when these changes require advance CAB approval and when they do not.

[Note: Any changes to a live application can only be implemented by a member of the IM (Information Management) team who will have access to live via a live deployment account]

If the raiser is not sure about the implementation of a change they should refer it to a senior or technical lead, who will advise if the change should go through the CAB.

1. Low impact and complexity Changes - eg. Data / Master Data / Bulk data / Reporting changes / Hotfixes

These are changes that have been successfully developed, tested and signed off on a test database (eg. QA), and are implemented by the IM team on the live system. All data changes must be recorded on an RFC (previously the central SITS change log) and receive appropriate peer review and approval (by suitable peer, senior technical lead). The RFC should be forwarded to the Change Manager by email for communication. No advance CAB approval is required to allow implementation of these. Retrospective review will take place and feedback given to raiser as required. They will be reviewed to ensure appropriate usage of this fastpath route.

Note: -Master Data:- The user community are currently (as of 12/09/2012) engaged in Master data changes (eg. Changing codes) and will need to be engaged in order to achieve success in controlling these changes.

Bulk Data:- IT Services performing the Bulk data updates will be advised of the updated process.

Hotfixes should now (as of Sep 2012) follow the same process as data/reporting changes. These were previously recorded on the hotfix log.

2. Application code changes (Tend to be Developmental or Functional Changes)

All other Application change should go to the CAB for approval via the current change process. Additional peer review is proposed. These changes will typically include:

- Project Implementations
- Operational Code changes
- Functional Changes
- Changes involving major upgrades
## 10.0 APPENDIX B: Risk Issues Template

### Risk Ratings as at: 12-Jul

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Risk Owner</th>
<th>Description of the Risk</th>
<th>Description of the Impact</th>
<th>Description of the Mitigation Strategy (and history)</th>
<th>Probability</th>
<th>Impact</th>
<th>Current Risk Rating</th>
<th>Risk Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

KEY: 'Office Use Only'

**Aggregate Risk Score:** 0

**Number of Risks:** 0

**Average Risk Score:** #DIV/0!

### Issues as at: 12-Jul

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Raised By</th>
<th>Description of the Issue</th>
<th>Action Taken and Planned</th>
<th>Urgency</th>
<th>Initial Action</th>
<th>Action Goal</th>
<th>Status</th>
<th>Date Open</th>
<th>Days Open</th>
<th>Days Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 11.0 APPENDIX C: Version of Process Document

<table>
<thead>
<tr>
<th>Version of Document</th>
<th>Process Document</th>
<th>Date Reviewed</th>
<th>Modifications made</th>
<th>Review Conducted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td></td>
<td>30 October 2009</td>
<td>Emergency change authorisation</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>3.1</td>
<td></td>
<td>April 2010</td>
<td>Updates from change review</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>3.1.1</td>
<td></td>
<td>October 2010</td>
<td>Updates from change review</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>3.1.2</td>
<td></td>
<td>April 2011</td>
<td>Introduce dutymanager role</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>3.1.3</td>
<td></td>
<td>October 2011</td>
<td>Updates from change review</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>4.0</td>
<td></td>
<td>April 2012</td>
<td>Updates from change review</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
<tr>
<td>4.1</td>
<td></td>
<td>October 2012</td>
<td>New change type of ‘Data’ and associated process</td>
<td>Louise Walsh (Quality Manager)</td>
</tr>
</tbody>
</table>