Change Management

Change Management Contents

Key

Glossary term: Glossary term

Cross reference: Cross reference

Becta ICT Advice

Change Management

Publication date March 2004
Originally published online in September 2003 as part of the Becta website
http://www.becta.org.uk/tsas

Becta
ICT Advice
British Educational Communications
and Technology Agency,
Millburn Hill Road,
Science Park,
Coventry CV4 7JJ

Change Management

ChM 1 Introduction to Change Management

Is making changes to your ICT giving you a headache? If so, FITS Change Management is for you…

ChM 1.1 Aim

The aim of this section is to introduce Change Management and to help you implement the process in your school with a minimum of preparation and training.

ChM 1.2 Objectives

The objectives of this section are to enable you to:

- understand the concept and benefits of Change Management
- understand what is involved in the process of Change Management
- understand the roles and responsibilities in Change Management
- implement a basic Change Management process in your school
- continue to operate this Change Management process
- identify useful measurements to gain benefit from the Change Management process you have implemented
- review your implementation and summarise your progress.

ChM 2 Overview

ChM 2.1 What is Change Management?

Change Management is the process for managing the implementation of changes to the ICT infrastructure including hardware, software, services or related documentation. Its purpose is to minimise the disruption to ICT services caused by change and to ensure that records of hardware, software, services and documentation are kept up to date.

In FITS Change Management, a change may be the result of a technical failure or problem and the nature and content of the change would be identified in the Problem Management, Availability Management or Capacity Management process. Alternatively a change may be the result of a new ICT software or hardware requirement. In this instance the Release Management process would be the mechanism for defining and developing the new service and ensuring its readiness for implementation. The Change Management process enables the actual change to take place and elements of the process include impact assessment, approval, scheduling, implementation and communication.

Some examples of changes are:

- updating a failed desktop PC
- installing a new software application
- assigning a software licence to a different user
- installing additional memory in a server
- revising a procedure document.

ChM 2.2 Why use Change Management?

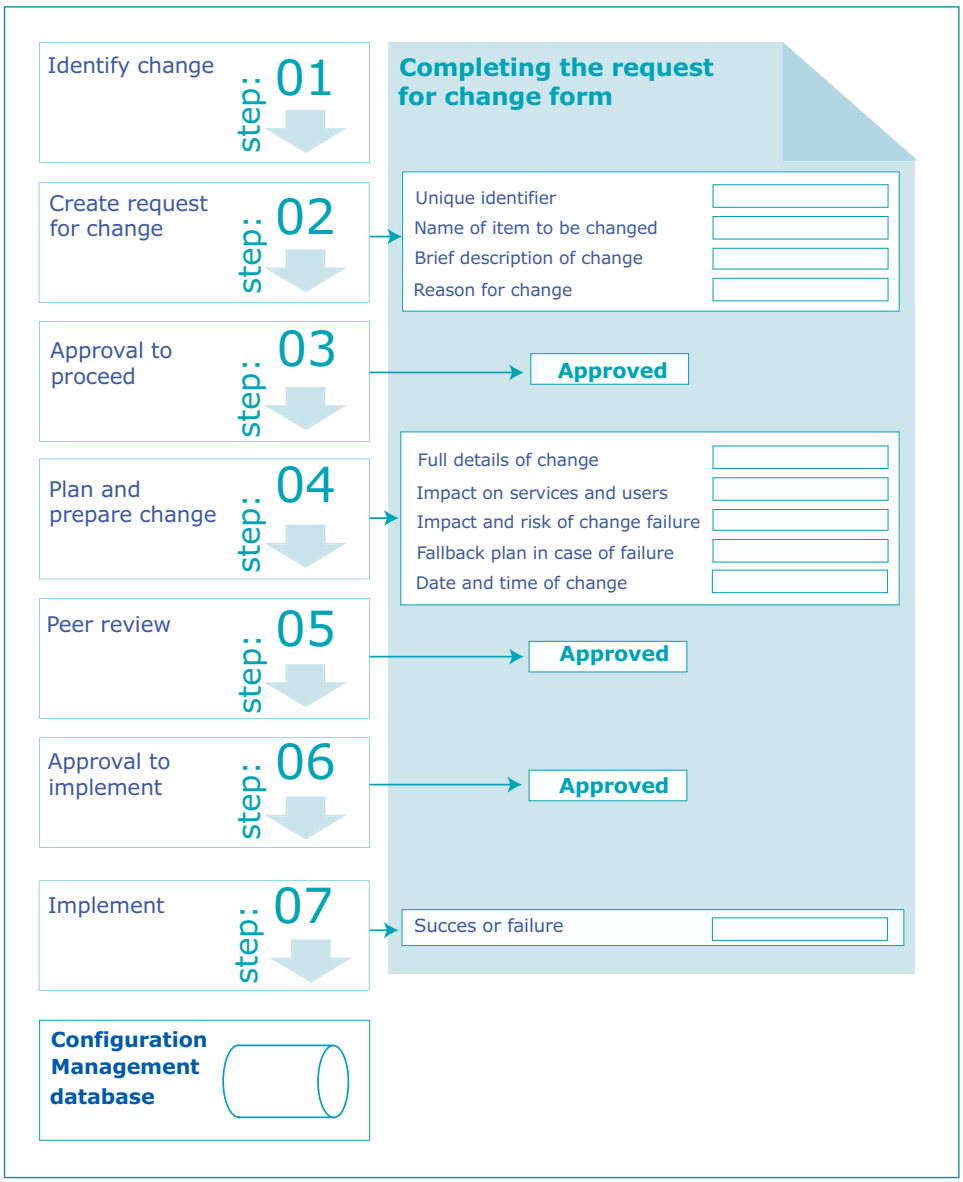
Change Management is proactive technical support focused on preventing incidents and problems by effective planning. Some of the benefits are:

- consistent planning for change
- consistent planning in case of failure of change
- communication with appropriate parties before change occurs
- approval received from appropriate parties before change occurs
- reduction in incidents and problems caused by unplanned change
- time spent on preparation and prevention rather than fire fighting and downtime.

ChM 2.3 Who uses Change Management?

Change Management is used predominantly by those responsible for ICT and ICT technical support.

Representatives of the user community may also be involved to give their perspective on changes to services and the scheduling of changes.



ChM 2.4

How Change Management works

Change Management works essentially by carrying out consistent planning, communication, approval and scheduling of change using a repeatable process and involving regular contributors. The Change Management process flowchart (above) illustrates this.

The process can be applied to all changes including individual user requests, or it can be applied just to major infrastructure changes that affect more than one user. We recommend that you apply it to major changes only, and for this reason user change requests are dealt with separately in Incident Management.

The Change Management process is enabled by a 'request for change' document to record the change details and approvals and an optional change advisory committee.

Request for change*	A request for change is completed for each change, with different roles contributing at different stages. It provides a checklist of items to be considered and approved before implementing a change. See Appendix A for our example request for change. As long as communication between the parties is effective and timely, you may be able to manage changes using only the request for change. Alternatively you may find it easier to gather approvers together on a regular basis for the purpose of approving changes and hold a change advisory committee meeting (see below). Requests for change are also used as input to the Configuration Management process to ensure that infrastructure records are kept up to date.
Change advisory committee	A change advisory committee is a regular meeting attended by key representatives in the Change Management process. It is a forum for the review and approval or rejection of proposed changes and change plans and is usually minuted.

* Not to be confused with a user request for a change to their computer or other personal ICT facilities. This is initiated using the incident/request form and its application is described in Incident Management. The request for change form referred to here relates to changes to shared ICT infrastructure that are initiated by ICT staff, although these may be as a result of a user incident or request.

ChM 2.5

What does Change Management cost?

The cost of change management has three aspects: expenditure, people and time.

In expenditure terms there is a cost only if you purchase software designed to aid the creation and processing of requests for change. We recommend that you do not purchase software at this stage but use the templates we have created for you to download. The implementation and operations guides refer to the templates as you need them, and we have also grouped them together in the appendices.

In people terms Change Management requires full-time change specialists only if there is a large volume of continuous change, usually in large organisations. In a school you should be able to allocate the roles and responsibilities to existing members of staff. Roles and responsibilities are referred to throughout the Change Management section, and also grouped together in ChM 5 Roles and responsibilities.

The amount of time taken up by the Change Management process once it is operational is difficult to quantify, as it will depend on the volume of changes in your school. There is a trade off between spending time planning and preparing changes thoroughly and making changes without planning that may result in incidents and problems later. We think prevention is better than cure!

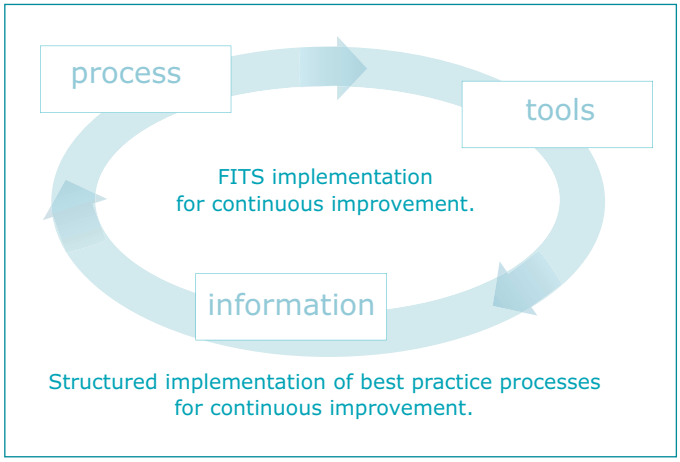
Remember to allow time also for the implementation and integration of the process into normal day-to-day activities. We have created a table of activities to help you plan the amount of time required.

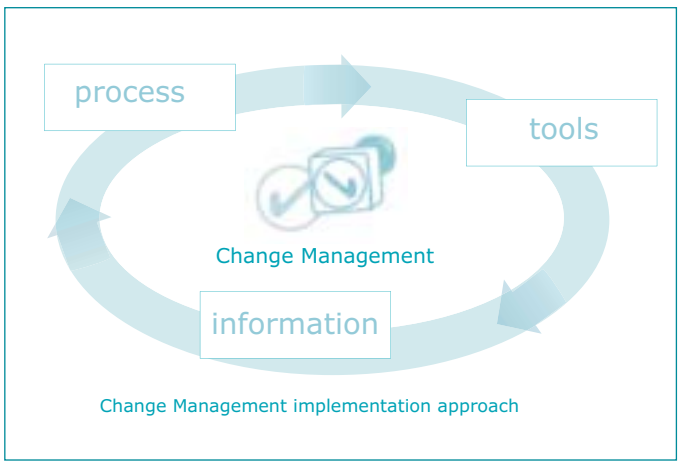
Activity	Example	Further information
Preparing for implementation	Discussions, planning	ChM 3 Implementation guide
Implementation	Training, pilot, actual implementation	ChM 3 Implementation guide

Activity	Example	Further information
Review of implementation	Difficulties with process or roles	ChM 3 Implementation guide
Raising requests for change	Planning changes, completing forms	ChM 4 Operations guide
Reviewing requests for change	Circulating forms, approvals	ChM 4 Operations guide
Administering change advisory committees	Agenda, minutes, meeting time	ChM 4 Operations guide

ChM 3 Implementation guide

ChM 3.1 Define what needs to be done





The FITS ethic is 'keep it simple' FITS also promotes a cyclic approach to its implementation: start small and make continuous improvements.

This first set of material introduces the processes with easy to follow instructions and simple tools to use. When you have implemented the processes, you will use the tools to gather information to make further improvements and thus enter the next cycle.

This process of refinement allows you to implement best practice in manageable, bite-size pieces. You will therefore reap the benefits from an early stage and not be overwhelmed by extra work.

Process

Implement Change Management process for major changes only and test process in a small group:

- raise Requests for Change for shared infrastructure items such as servers
- limit the number of process participants as far as possible.

Tools

Keep tools simple and requiring minimum effort:

- use Word template Request for Change and keep signed hard copies
- use Excel template for report.

Information

Start to gather data immediately to demonstrate progress, and produce monthly report including:

- total number of Requests for Change
- number of approved Requests for Change
- number of rejected Requests for Change
- number of successfully implemented changes
- number of failed changes.

As described in the overall FITS implementation approach, we recommend a cyclic approach to implementing new processes. Start small and build upon solid foundations.

FITS Change Management is for people with little free time to spend on implementing processes and procedures and whose day-to-day activities are unpredictable and must take priority.

Our aim is to help you begin to remove some of the unpredictability by introducing best-practice processes in small steps and so begin to realise the benefits as quickly as possible.

Long-term scope

Ultimately, Change Management should apply to all changes, from those affecting all or many users such as a server upgrade, to small individual changes, such as installing an application on a single computer. This ensures that there is a consistent mechanism for keeping inventory records up to date. This aspect of best practice is covered in more detail in Configuration Management.

Applying the disciplines of Change Management to all changes also encourages consistent and rigorous planning so reduces the likelihood of incidents following a change. However, to implement Change Management to this extent is time consuming.

Short-term scope

In the short term it is advisable to start in a small and manageable way and build gradually on solid foundations. We recommend that in the first instance you apply Change Management only to major changes that affect more than one user, such as the installation or upgrade of a server or a change to the network configuration. For this reason we have covered the handling of individual user requests in Incident Management. We also recommend that you approve requests for change as required and avoid the need for a change advisory committee at least at first.

The implementation guide will take you through the steps required to introduce Change Management in your school.

ChM 3.2 Prepare to implement

Good preparation can make the difference between a successful implementation of a process and an unsuccessful one.

Roles and responsibilities	The first step is to identify the process participants and assign roles and responsibilities. We recommend that for the initial implementation you involve as few people as possible so that the tasks can become familiar with minimum impact on the day-to-day workload of the school. The people you select to fulfil the Change Management roles will depend on how you currently provide technical support and who is involved already. ChM 3.2.1 Assigning roles and responsibilities in Change Management offers some suggestions and guidance.
Training	After you have assigned roles and responsibilities, it is important to ensure that those participating in the implementation and subsequent operation of the process understand what is required of them. Use the FITS website as training material.
Start date	Set a start date. A 'go-live' date is important in any implementation. Make sure that you allow enough time to do all the other preparatory tasks before your go-live date.

Communication	Communication must take place within the implementation team to agree plans, schedule dates and so on, but it is also important to communicate externally and inform the user community of the new process. The implementation of a process can be seen as a change just like the upgrading of a server and the impact on the user community should be communicated to them clearly in advance of the change.
Materials	Before you can go ahead with the implementation, you will need all the materials required for the process. Make sure that you have downloaded the templates you need and that everyone involved has access to them.
Pilot	Carry out a pilot implementation first as a test. To do this, complete a request for change for one change to familiarise the participants with the process. Then conduct a review and discuss any issues. When you are happy that everyone understands the requirements and that all roles are adequately fulfilled, you can raise a request for change for all changes as they arise.

ChM 3.2.1 Assigning roles and responsibilities in Change Management

Role	Suggested representative(s)	Comments
Originator	Person responsible for carrying out technical changes, eg: • technician • ICT co-ordinator • network manager • supplier.	You can have as many originators as there are people responsible for technical change.
Initial approver	Person who manages technical support or ICT, eg: • ICT manager • ICT co-ordinator • network manager • ICT teacher.	It is likely that there will be only one initial approver in a school. This will be the person who is responsible for the management of ICT.
Peer reviewer	Technical person who can confirm that the change plan is technically sound and appropriate, eg: • another technician • network manager • supplier • technician from another school.	The peer reviewer should be someone other than the originator, as they are reviewing the originator's change details. It is permissible to omit the peer review step from the process when initially implementing Change Management, to simplify the process.

Final approver	Person who has authority or delegated authority to give the go-ahead to make the change as planned, eg: • headteacher • ICT manager • ICT co-ordinator • another teacher.	This could be anyone who is in a position to sanction the actual change and agree that the impact on the rest of the school is acceptable (for example, any system downtime required). This level of participation should eventually be extended to someone outside the ICT area.
Implementer	Person responsible for carrying out technical changes, eg: • technician • ICT co-ordinator • network manager • supplier • teacher.	You can have as many implement as there are people responsible for technical change. Implementers and originators can be the same person.

ChM 3.3

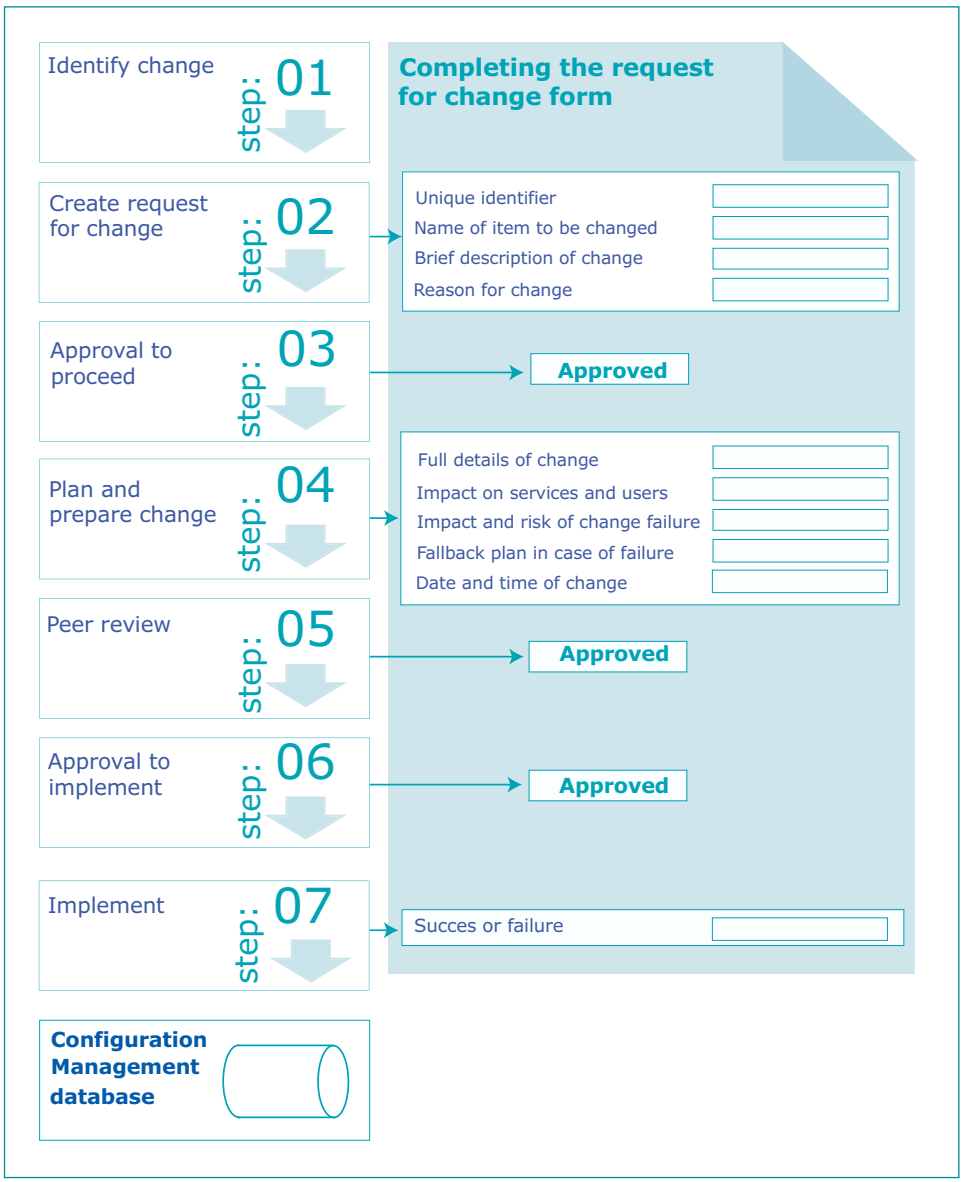
Implement

This section tells you how to create and complete a request for change and what to do with it at each stage of the process. After following the steps you will have implemented a basic Change Management process.

We have created a template request for change form that you may download and add to, or personalise with any existing additional steps you may already have in place – for example, additional approvers.

- Step 1: Identify change
- Step 2: Create request for change
- Step 3: Approval to proceed
- Step 4: Plan and prepare change
- Step 5: Peer review
- Step 6: Approval to implement
- Step 7: Communicatio
- Step 8: Implement
- Step 9: Update configuration-management database
- Step 10: Closure

There is also an optional section, ChM 3.3.1 Change advisory committee, which you may choose to implement or not, depending upon what is appropriate for your school.



Step 1 Identify change

First select the change to which the change management process will be applied.

In FITS Change Management a change is the result of:

- a problem requiring a change for resolution and that is affecting more than one user, such as a server hardware failure
- a new requirement as a result of advances in technology or needs, such as a software upgrade with new functionality.

A change may be identified by:

- a technician
- anyone responsible for ICT strategy.

Step 2 Create request for change

A new request for change should be created for each change. You must do this before you buy items or spend any time preparing the change, so that you can seek appropriate approval first.

The originator should create the request for change. A request for change in this context should not be confused with a user request for a change to their computer or other personal ICT facilities. This is initiated using the incident/request form and its application is described in Incident Management. The request for change form referred to here relates to changes to shared ICT infrastructure that are initiated by ICT staff, although these may be as a result of a user incident or request. End-users are not required to complete change management requests for change.

We have created a request for change template (see Appendix A) which you can download and use as it is or customise. See also Appendix A for our example request for change. The following sections on the request for change should be completed at this stage:

- Unique identifier
- Name of item to be changed
- Brief description of change
- Reason for change
- Originator and initial approver name

Unique identifier

The unique identifier is a reference that applies only to the item to be changed.

This may be:

- an asset tag number
- the serial number
- any other naming or numbering system in use by the school, such as room number and desk number.

For clarity, the unique identifier should be entered on the request for change form, especially if the make/model/type exists more than once.

Example:

Unique identifier	Asset tag 21383

Name of item to be changed

The name of the item to which the change applies should be entered on the request for change form.

This may be:

- make and model of computer, printer or other equipment
- name of application and version if applicable
- assigned name of equipment, such as file server name or printer queue name.

The purpose of this is to give a meaningful name to associate with the unique identifier, as it is unlikely that the unique identifier alone will immediately identify the type of equipment to the reader of the form.

Example:

Name of item	Compaq file server [server name], B Block computer room

Brief description of change

A brief description of the proposed change should be entered on the request for change.

This should include:

- nature of change
- any new equipment required
- any known costs
- estimated amount of time to plan and implement the change.

The purpose of this is to provide sufficient information to enable the initial approver to assess the cost in time and money of carrying out the change.

Example:

Brief description of change	Installation of Microsoft W2000 Server Service Pack 2

Reason for change

A brief description of the reason for the change should be entered on the request for change.

This may include:

- outline of problem to be resolved by change
- justification of need for new service
- if applicable, name of the person responsible for funding or departmental budget to be charged.

The purpose of this is to provide sufficient information to enable the initial approver to assess the value of carrying out the change.

Example:

Reason for change	Operating system patch available to fix bugs

Originator and initial approver names

- Enter the name of the originator (see ChM 5.1) so that approvers know whom to talk to if they require further information.
- Enter the name of the initial approver (see ChM 5.2) so that it is clear who is responsible for this level of approval.

Example:

Originator	Andrew Powell, Network Manager	
		Signatures
Initial approver	Debbie Wiggins, ICT Co-ordinator	

Step 3 Approval to proceed

Approval to proceed is granted (or not) by the initial approver, who must assess the cost and value of proceeding with the change. If insufficient information is on the request for change to enable the initial approver to make an assessment, they should refer back for further details to the originator, who must also update the request for change for the record.

This stage of approval is important, as it prevents time and money being wasted on activities that may be inappropriate in terms of strategy and the bigger picture. The initial approver (see ChM 5.2) has the power to approve, reject or place on hold proposed changes as they see fit and should have the appropriate level of authority.

Example:

Originator	Andrew Powell, Network Manager	
		Signatures
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins

Step 4 Plan and prepare change

Once approval to proceed has been granted, the originator may plan and prepare the change in earnest.

The following sections on the request for change must be completed at this stage:

- Full details of change
- Impact on services and users
- Impact and risk of change failing
- Fallback plan in case of failure
- Date and time of change
- Peer reviewer, implementer and final approver names

Full details of change

Full details of the change should be entered on the request for change.

This should include:

- plan for testing/testing carried out
- plan for implementation (steps to be taken, specific requirements for equipment and people, and so on)
- further timing details.

The purpose of this is to provide sufficient information to enable the peer reviewer and the final approver to assess the suitability and robustness of the change and plan before approving implementation.

Example:

Full details of change	• Check back-ups successful • Shut down server • Restart server • Login as admin user • Apply service pack from supplier • Execute upgrade • Restart server • Log in to server (test functionality and review error logs)

Impact on services and users

Details of the impact of the change on existing ICT services and users should be described.

This should include:

- whether or not the change will require downtime of existing services
- how long downtime will be for
- whether or not services may be disrupted during implementation of the change
- what services will be affected by downtime or disruption
- which users are affected
- whether or not timing of change reduces impact.

The purpose of this is to highlight the disruption to normal day-to-day activities that are likely to occur during implementation of the change and to enable the final approver to assess whether or not the disruption is acceptable.

Example:

Impact on services and users	• Server unavailable for one hour • Users unable to log in to computers for duration • ICT services unavailable for duration • Affects all users and services

Impact and risk of change failing

Details of the impact and risk of failure of the change should be outlined.

This should include:

- whether a failure of the change may result in an unplanned outage
- what services would be affected by an unplanned outage
- which users would be affected by an unplanned outage
- what the risk of failure is estimated to be (high risk or low risk)
- what has been done to reduce the risk (for instance, any testing that has been carried out)
- what risk mitigation has been carried out (such as a dry run of the installation using test equipment).

The purpose of this is to highlight the risks associated with the change if implementation does not go according to plan and to highlight the potential disruption to normal day-to-day activities.

Example:

Impact and risk of change failure	• Failure would require server rebuild and data restore • Estimated time to rebuild, restore and recover: 6 hours • Impact on services and users as above • Risk low – service pack released two months ago and no issues reported on the supplier's website

Fallback plan in case of failure

Details of a fallback plan for implementation in the event of change failure should be outlined.

This should include:

- what needs to be done to restore the service to its original state before the change was attempted
- what equipment or other resources are needed to be available to implement the fallback plan
- confirmation that equipment or resources have been arranged
- at what point the fallback plan will be invoked – for example, if work overruns and an unplanned outage is unacceptable.

The purpose of this is to demonstrate that a plan is in place for service recovery in the event of change failure. If a change fails, it is important that all original components are restored so that inventory records remain accurate. See Configuration Management for further details.

Example:

Fallback plan	• Restore operating system and data from tape • Restart server • Test server and data NB Tapes required on site in advance of change

Date and time of change

The date and time that the change will be implemented should be recorded on the request for change.

An estimate of the amount of time the change will take should also be included.

Example:

Date of change	Friday 25 April 2003
Time of change	1800 – 1900

Peer reviewer, implementer and final approver names

- Enter the name of the peer reviewer (see ChM 5.3) so that it is clear who is responsible for this level of approval.
- Enter the name of the implementer (see ChM 5.4) so that it is clear who will/did carry out the change.
- Enter the name of the final approver (see ChM 5.5) so that it is clear who is responsible for this level of approval.

Example:

Originator	Andrew Powell, Network Manager		
		Signatures	
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins	
Peer reviewer	James Burke, Supplier Representative		
Final approver	Debbie Wiggins (for Headteacher)		
		Success	Failure
Implementer	Andrew Powell, Network Manager		

Step 5 Peer review

On completion of the request for change, approval to implement is recommended (or not) from a technical perspective by the peer reviewer (see ChM 5.3), who must assess the change and implementation plan for technical suitability and robustness of solution. If insufficient information is on the request for change to enable the peer reviewer to make an assessment, they should refer back for further details to the originator, who must also update the request for change for the record.

Example:

Originator	Andrew Powell, Network Manager		
		Signatures	
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins	
Peer reviewer	James Burke, Supplier Representative	J Burke	
Final approver	Debbie Wiggins (for Headteacher)		
		Success	Failure
Implementer	Andrew Powell, Network Manager		

Step 6 Approval to implement

Following approval by the peer reviewer, ultimate approval to implement is granted (or not) by the final approver (see ChM 5.5). They should seek the views of affected or relevant user representatives to take part in this decision-making process. If insufficient information is on the request for change to enable the final approver to make an assessment they should refer back for further details to the originator, who must also update the request for change for the record.

Example:

Originator	Andrew Powell, Network Manager		
		Signatures	
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins	
Peer reviewer	James Burke, Supplier Representative	J Burke	
Final approver	Debbie Wiggins (for Headteacher)	D Wiggins	
		Success	Failure
Implementer	Andrew Powell, Network Manager		

Communication

It is important to communicate relevant details of the change to affected users. It is not necessary to distribute full technical details of the change, but those dependent upon the ICT services affected will appreciate a brief outline of the user impact.

A change communication should include:

- a simple description of the change, for instance installation of anti-virus software
- date and time of change
- services affected
- users affected
- nature of impact, such as complete outage
- duration of impact
- contact name and details for further information.

It is good practice to present such changes in a positive light by highlighting the benefits of the change (See Appendix D). It is also good practice to have a standard method for communication so that users can come to expect a similar format for everything related to ICT. It may be a good idea to make one person responsible for all communications. A consistent forum is also a good idea: for example, staff briefing meetings or intranet home page.

Step 7 Implement

Following final approval and after relevant and timely communications have been issued, the change may be implemented in accordance with the plan and the scheduled date and time.

It should be recorded on the request for change whether the change was successful or unsuccessful, so that it is clear from the record what the outcome of the request for change was.

Example:

Originator	Andrew Powell, Network Manager		
		Signatures	
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins	
Peer reviewer	James Burke, Supplier Representative	J Burke	
Final approver	Debbie Wiggins (for Headteacher)	D Wiggins	
		Success	Failure
Implementer	Andrew Powell, Network Manager	x	

Update Configuration Management database

Following successful change, inventory records should be updated to reflect the details. For example, if a file server is replaced and the old one is disposed of, the new file server needs to be recorded on the inventory with details such as make, model, serial number, asset tag number. Details of the old one must be removed.

The following are some examples of outcomes that may require inventory update:

- installing new hardware
- removing hardware
- installing new software
- reassigning a software licence to another user.

This activity forms part of the Configuration Management process, which is the subject of a separate section of FITS.

Closure

Congratulations, you have completed your request for change!

You should retain the signed paperwork for future reference.

ChM 3.3.1

Change advisory committee

A change advisory committee may be set up as a forum for the review and approval or rejection of proposed changes and change plans.

Membership of the change advisory committee should include but is not restricted to:

- Change manager, for example ICT manager or person responsible for ICT or technical support
- ICT technical representative, for example ICT manager or senior technical person

- strategic representative, for example headteacher
- user representative(s), for example ICT co-ordinator, teacher(s)
- other ad hoc representatives for specific changes as required.

Consensus may be achieved via a brief meeting that may be either scheduled to take place regularly or arranged as required. These should be treated as formal meetings (see below).

The change advisory committee is in addition to the request for change process and should be used only if it enhances the process. It may be helpful to have a regular meeting at which all changes are discussed and approved. But, depending upon the volume and frequency of changes, this may get in the way of change – which is not an acceptable feature of the process!

You may find it safer to consider each change as it arises, at least until the process is familiar, to avoid wasting time in unnecessary meetings and to avoid delaying changes. This also makes it easier to review emergency changes if all changes are dealt with as they arise.

Meetings

The change advisory committee meeting should approve or reject changes. The change manager should manage the meeting and facilitate agreement.

Creative use of technology can take the place of a physical meeting. For example, you could circulate requests for change and gather responses by email, or hold a virtual meeting via telephone conferencing. The latter methods can be particularly useful for gaining agreement in emergencies without taking up too much time and without having to wait for a meeting.

Agenda

A day or so before the meeting send out an agenda including hard copies of, or electronic links to, the requests for change to be discussed.

The membership should be asked to review all requests for change in advance of the meeting and be prepared with any questions or concerns. This ensures that the meeting is kept precisely for the purpose of approval or rejection and does not become a lengthy explanation of each change. If the details on a request for change are not self-explanatory, the request should be rejected before circulation.

See Appendix B for example agenda.

Minutes

A brief record of the outcome of change advisory committee meetings should be circulated for acceptance and kept for the record. These minutes should include approvals and rejections and any action points, those responsible for taking the actions and deadlines.

See Appendix C for example minutes.

ChM 3.4 Review the implementation

After you have completed your first request for change, ask some key questions and consider the answers before continuing to use the process:

- Did everyone understand what was required of them?
- Was each section of the request for change completed adequately?
- Does training need to be revisited before continuing?
- Were there any incidents as a result of the change?
- Were all interested parties aware of the change before it took place?

ChM 3.5 Implementation resources

For creating requests for change, use the request for change template (see Appendix A).

If you wish to implement a change advisory committee, the following templates may be useful:

- Change advisory committee agenda template (see Appendix B)
- Change advisory committee minutes template (see Appendix C)

ChM 4 Operations guide

ChM 4.1 What needs to be done?

The ongoing operational tasks for change management are:

- creating and approving requests for change
- communicating changes
- monitoring the Change Management process
- making decisions.

ChM 4.1.1 Creating and approving requests for change

A request for change should be completed for each change affecting the ICT infrastructure.

The request for change steps described in the implementation guide (see ChM 3.3) can be followed each time until everyone is familiar with the process and it becomes automatic. If you no longer need the instructions, you can download the request for change template (see Appendix A).

ChM 4.1.2 Communicating changes

It is a good idea to communicate planned changes to the ICT users, especially if system downtime is required. This communication can take the form of a regular documented summary of approvals and rejections, which may be distributed or pinned to notice boards.

Alternatively it may be more appropriate for the ICT technical support department to issue notification of downtime and impact specifically for each change to give appropriate warning. A combination of both methods is better if time permits.

Change communications should have a standard format with a clear layout so that readers can pick out relevant information quickly. See our example (Appendix D) for ideas.

It is also important that the service desk is made aware of change plans in advance of their being implemented. This will help the service desk to recognise related incidents if they occur and to deal with them efficiently and effectively.

ChM 4.1.3 Monitoring the Change Management process

It is important to quickly start to take regular measurements against all processes to plot how things change over time. When Change Management has been implemented, the following measurements should be easy to gather and report on using the information on the request for change forms:

- total number of requests for change
- number of approved requests for change
- number of rejected requests for change
- number of successfully implemented changes
- number of failed changes.

It is often worth while to publish reports on notice boards and/or issue them to key staff. This gives visibility of the workload of the department. But bear in mind that fluctuations will probably generate some questions, so understand the causes before you go public.

To get started on some simple measurements and reporting, download a Change Management report template with graphs produced in Excel (see Appendix E). Follow the instructions to fill in your volumes of requests for change and set the print range around the commentary and graphs before printing.

ChM 4.1.4

Making decisions about change management

The reports produced from the Change Management process output will enable you to monitor trends and look more closely for reasons for noticeable fluctuation. We give below some possible examples.

- A change in the volume of requests for change being raised may indicate growing or reducing problems, or a growth in need for ICT systems in general.
- A fluctuation in the volumes of approved or rejected requests for change may indicate difficulties in operating the Change Management process itself or it may be relative to the fluctuating number of requests for change.
- A fluctuation in the number of successful or failed changes may indicate issues with the planning process or may be relative to the number of requests for change.

The measurements you have gathered are to give an indication of areas in which to look for problems; they are not a solution in themselves. Identify trends and ask questions, look back through incident records, talk to the service desk staff. Dig around for the root cause. It is also important to identify and resolve issues with the process to ensure that the process continues to operate effectively.

ChM 4.2 When does it need doing?

Creating and approving requests for change	The frequency of creating requests for change will depend on the amount of change you undertake. It is good practice to use the request for change cycle (see ChM 4.1.1) as a way to trigger the appropriate planning stages. It is appropriate, therefore, to begin a request for change as soon as a change is identified and add to it as the plan develops. For the request for change template, see Appendix A.
Communicating changes	ICT system users should be given as much advance warning of ICT system downtime as possible in order to minimise disruption to their work and plans. It may also be a good idea to issue a reminder shortly before the downtime. The service desk staff also should be given as much notice as possible, as the potential impact of the change may have a direct effect on their plans and workload.
Monitoring the Change Management process	Measurements can be taken and reported weekly if you have a lot of changes, or monthly if there are not so many. It is important to be consistent in frequency so that the emerging trends are not distorted. The frequency can be reviewed and changed, but it is best not to switch randomly between weekly and monthly.
Making decisions	Reports should be reviewed as frequently as they are issued and trends identified as they appear. Actual causes of trends will be easier to identify if the data is recent.

ChM 4.3 Who does it?

Creating and approving requests for change	The originator of each change is responsible for starting the request for change cycle each time and for seeing it through to closure. Originators, peer reviewers and implementers may vary from change to change, but it is likely that the approvers will remain constant.
Communicating changes	Communication to ICT users may be issued by anyone familiar with the change, providing the content of the communication is not too technical and does not include jargon. It may be appropriate for the person responsible for ICT or technical support to issue communications, or the person responsible may delegate the task to, for example, the service desk.
Monitoring the Change Management process	Reporting is the responsibility of the person responsible for ICT or technical support. However, they may delegate it to anyone who has access to completed requests for change.
Making decisions	The person responsible for ICT and/or technical support should make decisions about changes. Their decisions should be based on a combination of their interpretation of report data and the answers to any questions arising from that data. To that end they may need to include anyone involved in the provision of ICT and technical support in the decision-making process.

ChM 4.4 Operational resources

- Request for change template (see Appendix A)
- Change management report template (see Appendix E)

If you wish to implement a change advisory committee, the following templates may be useful:

- Change advisory committee agenda (see Appendix B)
- Change advisory committee minutes (see Appendix C)

ChM5 Roles and responsibilities

ChM 5.1 Originator

- Identifies the change
- Creates the request for change
- Plans the change
- Manages the request for change through to approval
- May be required to attend change advisory committee meetings
- May also be the implementer of the change
- Is a technical person

ChM 5.2 Initial approver

- Gives permission to plan the change
- Should be ICT manager or equivalent
- May be financially responsible
- May not be the originator
- Need not be technical

ChM 5.3 Peer reviewer

- Reviews the plan for change and technical details
- Checks the solution is suitable
- May not be the originator
- May be the implementer
- Is a technical person
- May be a supplier

ChM 5.4 Implementer

- Implements the change
- Updates the request for change with the outcome of the change
- May be the same person as the originator
- May be the same person as the peer reviewer
- Is likely to be a technical person

ChM 5.5 Final approver

- Has the final say as to whetherthe change can be carried out as planned
- Should be outside ICT technical support, for example head teacher
- Does not need to be technical
- Should be able to decide on behalf of entire school
- Will be a member of the change advisory committee if one is required

ChM 5.6 Change manager

- Vets requests for change for clarity and completeness before issuing to change advisory committee
- Issues the agenda and minutes for the change advisory committee
- Chairs the change advisory committee
- Is responsible for the minutes of the change advisory committee
- May delegate administrative tasks
- Is often the person responsible for ICT or ICT technical support
- Does not need to be technical

ChM 6 Review of Change Management

The purpose of this section is to help you review your implementation and ongoing operation of change management, check your understanding of the process, examine what a successful implementation should look like and consider what you have achieved by introducing it into your school. This will help you to assess how successful its introduction has been and point you back to the relevant sections in the Change Management process that you should revisit to make improvements, if these are necessary.

Start by reading the sections included in the recap of Change Management. When you have refreshed your memory and considered your own implementation alongside these descriptions, work through the checklist to identify any areas you should revisit and perhaps re-implement or reinforce.

ChM 6.1 Recap of Change Management

In Change Management we introduced the concept of planning and implementing technical changes in a consistent manner. We gave you an overview of the whole Change Management process and an implementation guide giving step-by-step instructions to help you implement a change management process that we believe is appropriate for the needs of schools. An operations guide gave you a list of ongoing activities required by the process in order for you to keep it going and reap the benefits. We described roles and responsibilities and offered guidance on how to assign roles. We removed anything non-essential to give you a lean process requiring the minimum of effort and resource.

Check your understanding of the process by going through sections Chm 6.1.1 to ChM 6.1.4 overleaf.

ChM 6.1.1 Change Management summary

Step	Tasks
Create a request for change form	Complete the initial details of the change with: • unique identifier • name • brief description of the change • reason for the change • the name of the person raising the request for change (the originator) • the name of the person who will authorise the change to be planned (the initial approver).
Seek approval to proceed with developing the change and spend any money that may be required	Submit the partially completed form to the initial approver for their review, comments if appropriate, signature and return. This step may result in changes or outright rejection if the initial approver does not agree with the change.

Step	Tasks
Plan and prepare the change	Add to the request for change document the details of your planning and preparation, as these become available, including: • full details of the change • the impact of the change on ICT services and end-users • the risk of the change failing and the impact of failure on ICT services and end-users • a fallback plan for use in case the change does fail • the date and time the change will take place • the name of the person who is checking and approving the technicalities of the change (the peer reviewer) • the name of the person carrying out the change (the implementer) • the name of the person who will give the final go-ahead to implement the change (the final approver).
Seek approval of the technical plan	Submit the form to the peer reviewer for their review, comments (if appropriate), signature and return. This step may result in changes being made to the plan until the peer reviewer is able approve it.
Seek approval to implement the change	Submit the form to the final approver for their review, signature and return. This step should not result in changes to the plan, as any issues relating directly to the change should have been identified and resolved as a result of the initial approval and peer review. However, the scheduling of the change must be agreed with the final approver so this element may require change at this stage.
Communicate the change with other technical staff and end-users	Notify everyone affected by the change of the scheduled date and time and the impact of the change. This may be done in writing or at staff meetings or both, as long as reminders are timely.
Implement the change	Carry out the change and, if necessary, invoke the fallback plan. Indicate on the request for change form whether the change was successful or not and sign it off as complete.
Update records of affected equipment on configuration-management database (CMDB)	Pass the completed request for change form to the CMDB administrator for them to update records of equipment affected by the change as appropriate. Depending on how roles have been assigned, the CMDB administrator may also be the implementer.

ChM 6.1.2

What you should expect now that you have implemented Change Management

- Technical changes do not occur randomly or without authorisation.
- All technical staff who implement changes are familiar with the request for change process and comply with it at all times.
- Budget holders are asked to authorise expenditure on changes before they take place.
- End-users are aware of planned changes before these happen.
- Supporting technical staff (such as service desk) are aware of planned changes before they happen.
- A culture is developing whereby technical change is considered with the interests of the school as a whole and carried out in a collaborative way.

ChM 6.1.3

What you should have achieved through Change Management

- There is a way of recording and keeping track of changes that are made.
- All major changes (changes to shared infrastructure items such as servers, routers, network cabling, other communications links and so on) are planned, approved and scheduled in accordance with the request for change process.
- A method for handling requests for change has been established – either by circulating the request for change to the participants in the process or holding regular meetings of a change advisory committee.
- Changes are implemented in a timely manner (the process doesn't get in the way of change).
- Information about the number of changes being made is available.
- Changes can be considered within the context of bigger scheme of things (the whole-school strategy/business plan) and you take the most appropriate action for the long term.

ChM 6.1.4

Benefits of having implemented Change Management

- You use the same format to plan all changes, so changes become quicker to implement.
- All changes have a fallback plan ready so that you can restore service quickly in case of failure.
- End-users and school leaders are aware in advance that changes are scheduled to take place so that they can plan their work accordingly.
- School leaders, budget holders or line managers have the opportunity to approve changes before you have done too much work on them, so that you can limit the resources spent on inappropriate activities.
- You reduce the number of incidents and problems caused by unplanned change, so need to spend less time on fire fighting.
- More attention to planning and preparation will reduce the number of incidents and problems.

ChM 6.2

Checklist

Use this checklist to identify any areas of Change Management that have not been entirely successful. Then reinforce them by revisiting and re-implementing the relevant section of the FITS process.

Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful
You have assigned roles and responsibilities.	ChM 3.2.1 Assigning roles and responsibilities in Change Management
Participants in the Change Management process understand it.	ChM 2 Overview of Change Management
Request for change forms are available.	Appendix A Request for change example and template
Request for change forms are completed for all major changes and the content enables approvers to understand and authorise the changes.	ChM 3.3 Implement request for change process Appendix A Request for change example and template ChM 4.2 When does it need doing? ChM 4.3 Who does it?
Changes are communicated effectively and consistently to those affected.	ChM 4.1.2 Communicating changes ChM 4.2 When does it need doing? ChM 4.3 Who does it?
Change management reports are produced regularly.	ChM 4.1.3 Monitoring the Change Management process ChM 4.2 When does it need doing? ChM 4.3 Who does it?
Change management reports are used to understand the use of the process, identify issues and make decisions.	ChM 4.14 Making decisions about change management ChM 4.2 When does it need doing? ChM 4.3 Who does it?

If the above characteristics are all true of your school, congratulations on implementing a successful change management process! The next steps for you are to continue operating the process as described in the Change Management operations guide (ChM 4) and establish the process firmly. Work through this checklist at regular intervals to help you check that everyone responsible continues to carry out all aspects of the process. You can then refer to the relevant sections to address any shortfalls as they arise.

Appendices

ChM Appendix A Request for change – example and template

Becta ICT Advice

Framework for ICT Technical Support (FITS)

Change Management

Example Request for Change

			task completed by
Unique identifier	Asset tag 21383		Originator
Name of item	Compaq file server [server name], B Block Computer Room		Originator
Brief description of change	Installation of server operating-system service pack		Originator
Reason for change	Operating-system patch available to fix bugs		Originator
Full details of change	Check backups successful Shutdown server Restart server Login as Admin user Apply service pack from supplier Execute upgrade Shutdown server Restart server Login to server (test functionality and review error logs)		Originator
Impact on services and users	Server unavailable for one hour Users unable to login to computers for duration ICT services unavailable for duration Affects all users and services		Originator
Impact and risk of change failure	Failure would require server rebuild and data restore Estimated time to rebuild, restore and recover: 6 hours Impact on services and users as above Risk is low – service pack was released 2 months ago and no issues have been reported on the supplier's website		Originator
Fallback plan	Restore operating system and data from tape Restart server Test server and data NB Tapes required on site in advance of change		Originator
Date of change	Friday 25 April 2003		Originator
Time of change	18:00–19:00		Originator
Originator	Andrew Powell, Network Manager		Originator
		Approval signatures	
Initial approver	Debbie Wiggins, ICT Co-ordinator	D Wiggins	Initial approver
Peer reviewer	James Burke, Supplier Representative	J Burke	Peer reviewer
Final approver	Debbie Wiggins (for School Head)	D Wiggins	Final approver
		Success Failure	
Implementer	Andrew Powell, Network Manager	✓	Implementer

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website **http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=change&id=tt5142**

Becta ICT Advice

Framework for ICT Technical Support (FITS)

Change Management

Example Change Advisory Committee Agenda

Date:	Tuesday 15 April 2003
Time:	10:00-10:30
Venue:	Room 2, Science Block
Distribution:	Mrs A Black, Headteacher Mr B White, Physics Teacher Miss C Green, Network Manager (Chair) Mr D Brown, ICT Co-ordinator (Minutes)

Item No.	Item description
1	Open meeting
2	Apologies for absence
3	Requests for Change for approval (papers attached) RFC123 – Data server disk upgrade RFC124 – Installation of network-monitoring software RFC125 – Withdrawn (additional ISDN line) RFC126 – Returned for further details RFC127 – Router move - review outcome
4	Changes scheduled this period – reminder
5	Date of next meeting
6	Any other business
7	Close meeting

Issued by:	Miss C Green Network manager and change advisory committee chairperson Friday 11 April 2003

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website **http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=change&id=tt5142**

Becta ICT Advice

Framework for ICT Technical Support (FITS)

Change Management

Example Change Advisory Committee Minutes

Date: Tuesday 15 April 2003
Time: 10:00-10:30
Venue: Room 2, Science Block
Distribution: Mrs A Black, Headteacher (AB)
Mr B White, Physics Teacher (BW)
Miss C Green, Network Manager (Chair) (CG)
Mr D Brown, ICT Co-ordinator (Minutes) (DB)

Request for Change No.	Description	Status
RFC123	Data-server disk upgrade	Initial approval
RFC124	Installation of network-monitoring software	Final approval
RFC125	Withdrawn (additional ISDN line)	Closed
RFC126	Returned for further details	Pending
RFC127	Router move	Successful -closed

Action owner	Action points	Date required
CG	Confirm time for server downtime on Thursday 17 April (RFC124) and issue notice to all staff	17 April 2003

Issued by:

http://www.becta.org.uk/techicalsupport/
published September 2003

You can download the template from the FITS website **http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=change&id=tt5142**

Becta ICT Advice

Framework for ICT Technical Support (FITS)

Change Management

Notification of ICT System Outage

To: All staff
From: ICT Technical Support
Date: 23 April 2003

Data-file server

This is to notify all ICT system users of a planned system outage:
Equipment affected: Data-file server
Date of outage: Friday 25 April 2003
Time of outage: 18:00-19:00
Log-out time: 17:45

This outage will affect all ICT users, who will be unable to access their computer files during this period.

This work is to enable the technical support department to apply new software designed to improve the reliability of the system, which will reduce the risk of unexpected failure in the future and improve the overall ICT service provided.

Please note that you are requested to save your work and log out of your computer by 17:45 on Friday to enable this work to be carried out on schedule. Please let me know if you anticipate this causing a problem.

Thank you very much in advance for your co-operation.

If you require further information, please contact me on extension 123.

Regards

Andy

Andrew Powell
Network Manager

http://www.becta.org.uk/techicalsupport/
published September 2003

Framework for ICT Technical Support (FITS)

Becta | ict advice

Change Management report: example

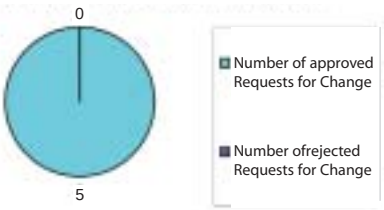
Enter Monthly volumes in the columns below

Enter current months in Current cells >	Current	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Number of approved Requests for Change >	5	1	3	5	1	2	10	3	5				
Number of rejected Requests for Change >	0	0	1	2	0	0	1	0	0				
Total number of Requests for Change >	**5**	**1**	**4**	**7**	**1**	**2**	**11**	**3**	**5**	**0**	**0**	**0**	**0**
Number of successfully implemented changes>	4	1	2	3	1	2	8	3	4				
Number of failed changes >	**1**	**0**	**1**	**2**	**0**	**0**	**2**	**0**	**1**				

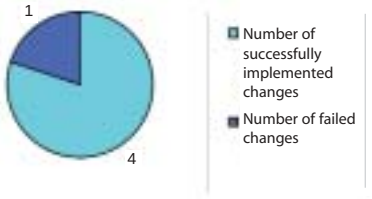
Save and print

This section of the report shows the total number of Requests for Change processed this month, both approved and rejected, and of those approved how many actual changes were successful or unsuccessful.

Volumes of approved and rejected Requests for Change this month

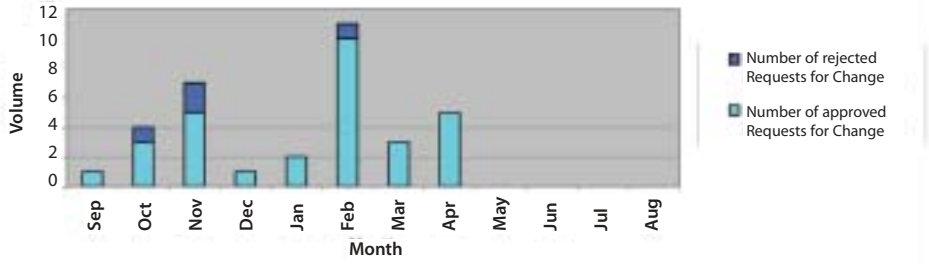


Volumes of successful and unsuccessful changes this month

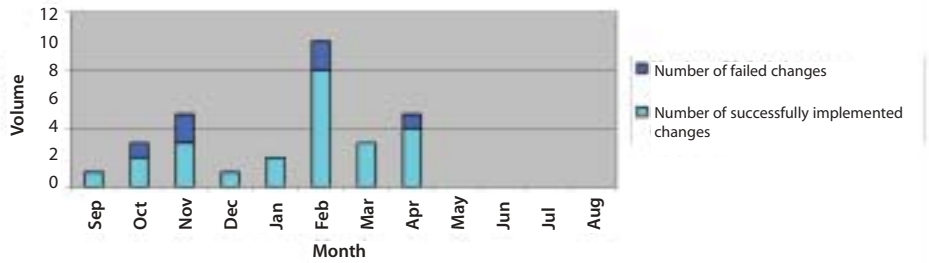


This section of the report shows the same figures plotted throughout the year:

Volumes of approved and rejected Requests for Change monthly to date



Volumes of successful and unsuccessful changes monthly to date



http://www.becta.org.uk/techicalsupport/
published September 2003

cm_report_example.xls
page 1 of 1

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=change&id=tt5142

Glossary

10Base-T	A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 10Base-T is based on the older Ethernet standard but is 10 times faster than Ethernet; it is often referred to as Fast Ethernet. Officially, the 10Base-T standard is IEEE 802.3u. Like Ethernet, 10Base-T is based on the CSMA/CD LAN access method.
AppleTalk	Inexpensive LAN (local area network) architecture built into all Apple Macintosh computers and laser printers. AppleTalk supports Apple's LocalTalk cabling scheme, as well as Ethernet and IBM Token Ring. It can connect Macintosh computers and printers, and even PCs if they are equipped with special AppleTalk hardware and software.
Asset	Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.
Availability	Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio: the proportion of time that the service is actually available for use by customers within the agreed service hours.
Availability Management	To ensure that ICT services are available for use consistently as agreed.
Bandwidth	The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps).
Baseline	A snapshot or a position which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position.
Bridge	A device that connects two LANs (local area networks), or two segments of the same LAN that use the same protocol, such as Ethernet or Token Ring.
Buffer	A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device.
Build	The final stage in producing a usable configuration. The process involves taking one or more input configuration items and processing (building) them to create one or more output configuration items (eg software compile and load).
Capacity	Ability of available supply of processing power to match the demands made on it by the business, both now and in the future.
Capacity Management	To ensure that all ICT processing and storage capacity provision match present and evolving needs.
Category	Classification of a group of configuration items, change documents, incidents or problems.
Change	The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

Change Management	The managed and recorded introduction of changes to hardware, software, services or documentation to minimise disruption to ICT operation and maintain accurate configuration information.
Client	The client part of a client/server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an email client is an application that enables you to send and receive email.
Client/server architecture	A network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers) or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources such as files, devices and even processing power.
Configuration management database (CMDB)	A database which contains all relevant details of each ICT asset, otherwise known as a configuration item (CI), and details of the important relationships between CIs.
Configuration Management	Implementing and maintaining up-to-date records of ICT hardware, software, services and documentation, and showing the relationships between them.
Definitive software library (DSL)	The library in which the definitive authorised versions of all software CIs are stored and protected. It is a physical library or storage repository where master copies of software versions are placed. This one logical storage area may in reality consist of one or more physical software libraries or filestores. They should be separate from development and test filestore areas. The DSL may also include a physical store (fire-proof safe, for example) to hold master copies of bought-in software. Only authorised software, strictly controlled by Change Management and Release Management, should be accepted into the DSL. The DSL exists not directly because of the needs of the Configuration Management process, but as a common base for the Release Management and Configuration Management processes.
Device	Any computer or component that attaches to a network.
Error trap	A signal informing a program that an event has occurred. When a program receives an interrupt signal, it takes a specified action (which can be to ignore the signal). Interrupt signals can cause a program to suspend itself temporarily to service the interrupt.
Ethernet	A LAN (local area network) architecture developed in 1976 by Xerox Corporation in co-operation with DEC and Intel. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet is one of the most widely implemented LAN standards.
FDDI (Fibre Distributed Data Interface)	A set of ANSI protocols for sending digital data over fibre optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for wide area networks.
Financial Management	To ensure that the ICT and technical resources are implemented and managed in a cost-effective way.

Firewall	A system designed to prevent unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorised internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
Gateway	A node on a network that serves as an entrance to another network. In schools, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving web pages. In homes, the gateway is the ISP that connects the user to the internet.
Gigabit	When used to describe data transfer rates, it refers to 10 to the 9th power (1,000,000,000) bits. Gigabit is abbreviated Gb, as opposed to gigabyte, which is abbreviated GB.
HTTP (hypertext transfer protocol)	The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the web server directing it to fetch and transmit the requested web page.
Hub	A connection point for devices in a network. Hubs are commonly used to connect segments of a LAN (local area network). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
ICT	The convergence of information technology, telecommunications and data networking technologies into a single technology.
Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.
Incident Management	To detect, diagnose and resolve ICT incidents as quickly as possible and minimise their adverse impact on normal operation.
ITIL	The OGC IT Infrastructure Library – a set of guides on the management and provision of operational IT services.
LAN	A computer network that spans a relatively small area. Most local area networks (LANs) are confined to a single building or group of buildings.
LocalTalk	The cabling scheme supported by the AppleTalk network protocol for Macintosh computers. Most local area networks that use AppleTalk, such as TOPS, also conform to the LocalTalk cable system. Such networks are sometimes called LocalTalk networks.
Logical topology	The logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.
MAC (media access control) address	Each device on a network can be identified by its MAC address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the data link control (DLC) layer of the OSI reference model is divided into two sub-layers: the logical link control (LLC) layer and the MAC layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.

Management information base (MIB)	A management information base (MIB) is a database of objects that can be monitored by a network management system. Both SNMP and RMON use standardised MIB formats that allow any SNMP and RMON tools to monitor any device defined by a MIB.
Network	A group of two or more computer systems linked together. The two types of computer networks of interest to schools are LANs (local area networks) and WANs (wide area networks).
Network interface card (NIC)	A network interface card (NIC) is an expansion board inserted or built into a computer so that the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol, although some can serve multiple networks.
Network traffic	The load on a communications device or system.
Node	A processing location. A node can be a workstation or some other device, such as a printer. Every node has a unique network address, sometimes called a data link control (DLC) address or media access control (MAC) address.
OSI reference model	The OSI (open system interconnection) model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station, and back up the hierarchy.
Packet	A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.
Packet switching	Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
Peer-to-peer network	A type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others.
Physical topology	The physical layout of devices on a network. Every LAN (local area network) has a topology – the way the devices on a network are arranged and how they communicate with each other.
Port	In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.
Problem	The underlying cause of an incident or incidents.
Problem Management	The detection of the underlying causes of incidents and their resolution and prevention.
Protocol	An agreed format for transmitting data between two devices.
Protocol stack	A set of network protocol layers that work together. The OSI reference model that defines seven protocol layers is often called a stack, as is the set of TCP/IP protocols that define communication over the internet.

Proxy server	A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server.
Release Management	To plan, test and manage the successful implementation of software and hardware. To define release policy and to ensure that master copies of all software are secured centrally.
Remote monitoring (RMON)	Remote monitoring (RMON) is a network management protocol that allows network information to be gathered at a single workstation. For RMON to work, network devices such as hubs and switches must be designed to support it.
Request for change	Form or screen used to record details of a request for a change to any CI within an infrastructure, or to procedures and items associated with the infrastructure.
Router	A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs (local area networks) or WANs (wide area networks) or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.
Segment	A section of a network that is bounded by bridges, routers or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN.
Server	A workstation or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.
Service Continuity Management	To minimise the impact on ICT service of an environmental disaster and put in place and communicate a plan for recovery.
Service Desk	The single point of contact within the school for all users of ICT and the services provided by Technical Support.
Service level agreement	Written agreement between a service provider and the customer(s) that documents agreed service levels for a service.
Service Level Management	The process of defining, agreeing and documenting required service levels and ensuring that these levels are met.
Simple network management protocol (SNMP)	A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in management information bases (MIBs) and return this data to the SNMP requesters.
Star topology	A LAN (local area network) that uses a star topology in which all nodes are connected to a central computer. The main advantages of a star network are that one malfunctioning node does not affect the rest of the network and that it is easy to add and remove nodes.
Switch	A device that filters and forwards packets between segments of a LAN (local area network). Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI reference model and therefore support any packet protocol.

TCP/IP (Transmission Control Protocol/Internet Protocol)	The suite of communications protocols used to connect hosts on the internet. TCP/IP uses several protocols, the two main ones being TCP and IP.
Token ring	A type of computer network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network.
Topology	The shape of a LAN (local area network) or other communications system. Topologies are either physical or logical.
User datagram protocol (UDP)	A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.
WAN	A computer network that spans a relatively large geographical area. Typically, a wide area network (WAN) consists of two or more LANs (local area networks). Computers connected to a wide area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the internet.
Workstation	Any computer connected to a LAN (local area network).