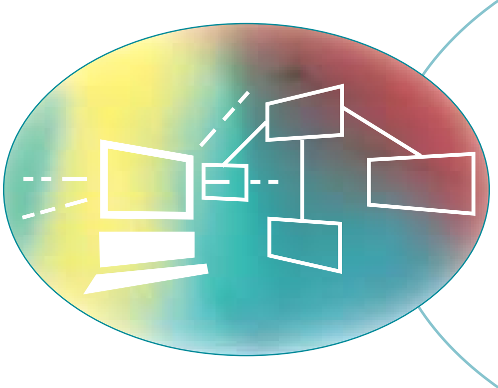


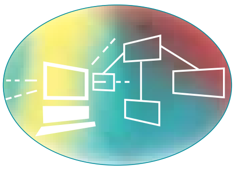
Configuration Management

Configuration Management Contents

Key

Glossary term:	Glossary term
Cross reference:	Cross reference

Becta
ICT Advice

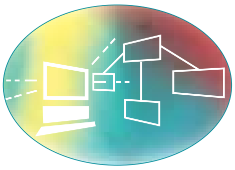


Configuration Management

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

While every care has been taken in the compilation of this information to ensure that it is accurate at the time of publication, Becta cannot be held responsible for any loss, damage or inconvenience caused as a result of any error or inaccuracy within these pages. Although all references to external sources (including any sites linked to the Becta site) are checked both at the time of compilation and on a regular basis, Becta does not accept any responsibility for or otherwise endorse any product or information contained in these pages, including any sources.

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



Configuration Management

CoM 1 Introduction to Configuration Management

Would you like to have up-to-date ICT equipment information at your fingertips? FITS Configuration Management helps you to achieve that, and more…

CoM 1.1 Aim

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

CoM 1.2 Objectives

The objectives of this section are to enable you to:

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

CoM 2 Overview

CoM 2.1 What is Configuration Management?

Configuration management is the process of creating and maintaining an up-to-date record of all the components of the ICT infrastructure, including related documentation. Its purpose is to show what makes up the ICT infrastructure and illustrate the physical locations and links between each item, known as configuration items.

Configuration management is more than just the recording of computer hardware for the purpose of asset management, although it can be used to maintain asset information. The extra value provided by configuration management is the rich source of support information it provides consistently to all interested parties. This information is stored together in the configuration management database.

CoM 2.2 Why use Configuration Management?

Configuration management is proactive technical support focused on providing information to help resolve incidents and problems. Some of the benefits are that:

- technical information is available to ICT staff and suppliers
- dependencies between configuration items are understood
- the information available helps in the planning of changes
- there is a single, therefore consistent, source of information
- graphical representation of infrastructure is available to aid diagnosis of incidents and problems

- when supported by Change Management, the configuration management database information is kept up to date (see CoM 2.4.1)
- it provides an asset list.

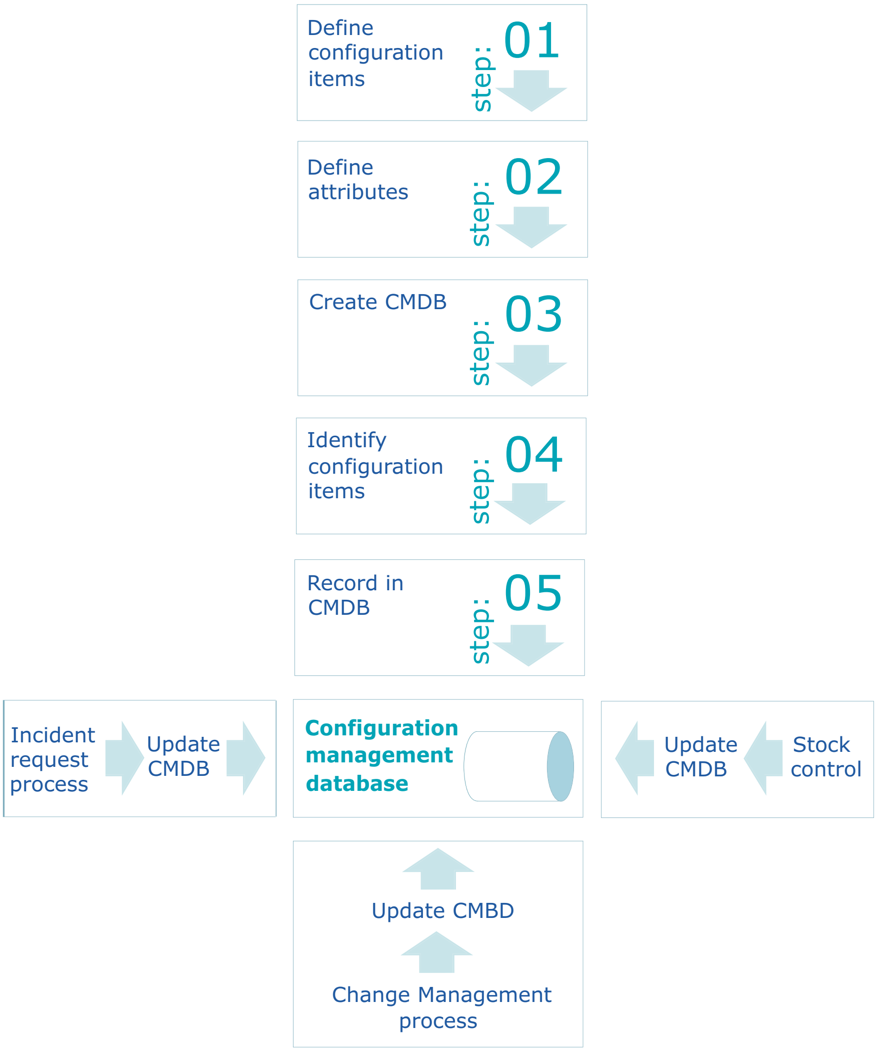
CoM 2.3 Who uses Configuration Management?

Configuration management is used predominantly by those responsible for ICT and ICT technical support. These may include external suppliers.

Access to asset information may be required by those responsible for the finances of the school.

CoM 2.4 How Configuration Management works

Configuration management works by identifying configuration items and their inter-relationships, recording them and keeping them up to date. The Configuration Management process flowchart illustrates this.



Configuration Management process

The process is enabled by a configuration management database (CMDB) to record the configuration items. This is kept up to date via its relationships with other processes.

CoM 2.4.1

Configuration management database

The configuration management database (CMDB) is where all information on configuration items is stored. The data is made up of configuration item records and attributes of those records.

Configuration items

Configuration items are the different components of the infrastructure that make up the whole, including associated items such as documentation, manuals, procedures and licences. For example configuration items, see Appendix A.

It is possible to record configuration items at various levels of detail. For example, you may choose to capture a large amount of detail and decide to record each individual computer base unit, monitor, keyboard, mouse, internal modem and so on as separate configuration items. You would do this if it were of importance to know where every single component is.

Alternatively you may choose to record only computer base units, as it can be assumed that the peripherals are bound to be present. You could then limit your records about peripherals to stock control only.

Attributes

In addition to the multitude of configuration items you will record, each item has a set of attributes. An attribute is a piece of information relating to the configuration item and these attributes can be as many or as few as you wish. For example attributes, see Appendix B.

When deciding at what level to record configuration items and how many attributes to include, the key factors to take into account are maintainability and need.

Maintainability

The more detail you record, the more there is to keep up to date and the more likely it is that it will become out of date.

Need

Record only what you need to know. Don't keep records for the sake of them. If you know that there is a computer base unit in a classroom, you know that it must have a keyboard, monitor and mouse. It is only if you have specialist peripherals that you may need to record more information.

Record only what is individual to each configuration item. If you have a maintenance contract for all your hardware, the supplier's contact details will be the same for every item so consider keeping that information centrally elsewhere.

Holding this information all together in a central database enables a number of different interfaces to be created – for example:

- a call-logging screen for recording incidents against configuration items
- a request for change screen for raising requests for change against configuration items.

This creates a powerful information tool.

CoM 2.4.2 Relationships with other processes

Relationship with Change Management	Change Management is the process for managing the implementation of changes to the ICT infrastructure including hardware, software, services or related documentation. It can be used to help maintain the configuration management database, as the final step in the request for change cycle is to update the configuration management database following a change. Change Management is the subject of a separate FITS section.
Relationship with Incident Management	Incident Management is the process for handling all user incidents, including equipment faults, and all requests, including those for new equipment. It can be used to help maintain the configuration management database, as the final step in the incident/request process is to update the configuration management database following a change. Incident Management is the subject of a separate FITS section.
Relationship with stock control	Either the Change Management process or the Incident Management process should capture most inputs to the configuration management database. The only occasion when there may not be a request for change or an incident/request sheet may be the procurement of stock items not initiated by an incident, request or change. It is important that the goods-in process feeds into configuration management immediately on receipt, so that new equipment is traceable before it is assigned to a location or user. Stock control is discussed in more detail in CoM 3 Implementation guide.

CoM 2.5 What does Configuration Management cost?

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

In expenditure terms the cost is focused on the purchase of software to create a configuration management database. At the sophisticated end of the scale it can be costly to provide the dynamic functionality required to view relationships between configuration items. It may also include aspects of the service desk, change management, incident management, problem management and release management. It takes some time to reach the point where this level of sophistication is needed and we recommend that you do not purchase software at this stage, but use the templates we have created for you to download. The implementation guide and operations guide of each process refer to templates as they are required. Examples and templates are also grouped together in the appendices.

Configuration management requires full-time staff only if there is a large volume of continuous change – usually only 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 Configuration Management section and they are also grouped together in CoM 5 Roles and responsibilities.

The amount of time taken up by the Configuration Management process once it is operational is difficult to quantify, as this will depend on the volume of changes in your school. Spending time proactively on a configuration management database and keeping it up to date can save time and effort spent later trying to track down equipment or trying to understand the infrastructure. Proactive is better than reactive!

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.

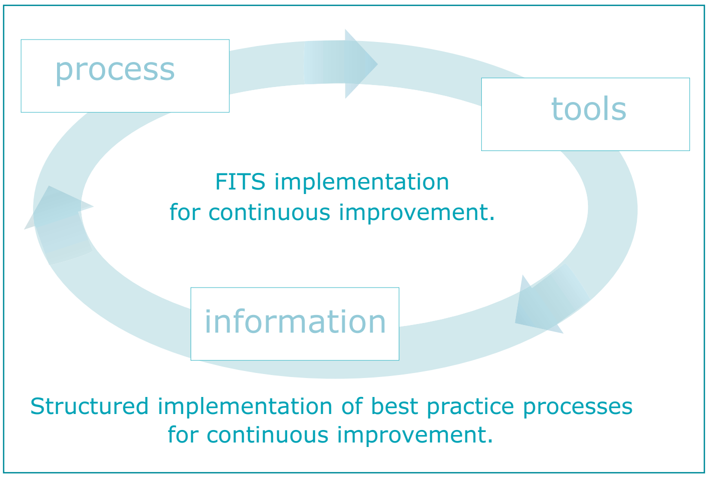
Activity	Example	Further information
Preparing for implementation	Discussions, planning	CoM 3 Implementation guide
Implementation	Training, pilot, actual implementation	CoM 3 Implementation guide
Review of implementation	Difficulties with process or roles	CoM 3 Implementation guide
Processing changes	Handling requests for change and incident/request forms	CoM 4 Operations guide
Updating the configuration management database	Adding, moving and deleting configuration items and maintaining their attributes	CoM 4 Operations guide
Auditing	Carrying out periodic checks to verify the accuracy of the configuration management database	CoM 4 Operations guide
Monitoring the process	Reporting against the process and ensuring that it is effective	CoM 4 Operations guide

CoM 3 Implementation guide

CoM 3.1

Define what needs to be done

As described in the overall FITS implementation approach, we recommend a phased approach to implementing new processes.


process
tools
FITS implementation
for continuous improvement.
information
Structured implementation of best practice processes
for continuous improvement.

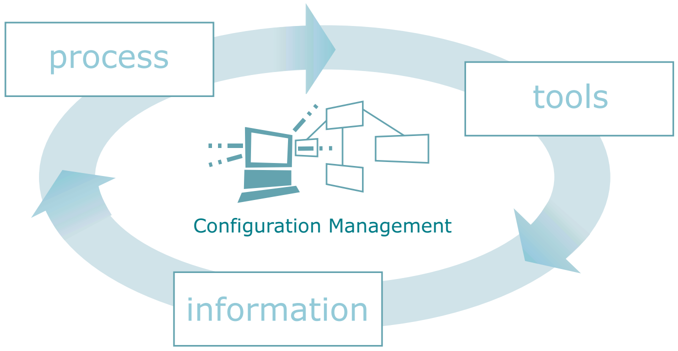
The FITS ethic is 'keep it simple'. FITS also promotes a cyclic approach to its implementation: start small and make continuous improvements.

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.

FITS Configuration 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.



Configuration Management implementation approach

Process

Implement Configuration Management process to record and maintain configuration items with limited attributes

- Identify configuration item level and attributes
- Audit all equipment
- Record all equipment
- Manage all changes
- Limit the number of process participants as far as possible

Tools

Keep tools simple and requiring minimum effort

- Use Word template request for change form
- Use Word template incident/request sheet
- Use Excel template for CMDB

Information

Start to gather data immediately to demonstrate value and produce regular audit report including

- Number of configuration items recorded in CMDB
- Number of physical configuration items
- Number of incorrect records in CMDB

Long-term scope

In the long term, configuration management should provide a detailed and accurate virtual representation of the services, equipment and associated documentation in the ICT infrastructure. This representation should also illustrate the relationships between these items. This model of the ICT infrastructure, providing it is kept up to date, enables decisions to be taken, plans to be made, problems to be diagnosed and actions to be performed without having to carry out a real-time investigation into what connects to what, etc.

However, for it to be fully effective, this is complex and time consuming. Being over-ambitious at the start may mean early failure of the process and wasted time and effort.

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 first you establish the maintenance processes (Change Management and the incident/request process) and then implement a configuration management database, using basic tools with carefully defined configuration items and minimal attributes. This will ensure that the database does not contain so much data that it is impossible to maintain with the resources available, yet establishes a foundation of useful information on which to build.

Our implementation guide will take you through the steps required to introduce Configuration Management in your school, including recommended configuration items and attributes to keep it manageable.

CoM 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 for initial implementation you involve as few people as possible in the process so that it can become familiar with minimum impact on the day-to-day workload of the school.

The people you select to fulfil the configuration management roles will depend on how you currently provide technical support and who is involved already. CoM 3.2.1 Assigning roles and responsibilities in Configuration Management offers some suggestions and guidance.

Further details of the roles and responsibilities can be viewed in CoM 5 Roles and responsibilities.

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 and its benefits to them.

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. They will more readily embrace it if they are not taken by surprise.

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 as a test first.

Create a dummy configuration management database and enter a couple of records. Use the incident/request process and the Change Management process to generate a test update to the dummy database.

Before gathering the initial data and populating the live database, check that the incident/request and change management processes work as a means to update the CMDB. The mechanism for maintaining the configuration management database is vital to its value – if the update processes don't work, the CMDB will soon become out of date.

Prerequisites

The implementation guide links closely to the operations guide in that the operational processes required to maintain the configuration management database must be in place before the CMDB is populated. Failure to do so will result in a CMDB that becomes quickly inaccurate. The only solution to this is to do a complete audit of equipment and recreate the CMDB.

For further information about the relationships between processes and a recommended order of implementation, see FITS 5.1.1.1 Recommended path for established technical support and/or ICT functions and FITS 5.1.1.2 recommended path for new ICT and technical support functions.

CoM 3.2.1 Assigning roles and responsibilities in Configuration Management

Role	Suggested representative(s)	Comments
CMDB administrator	An administrative or technical person with access to the configuration management database, eg: • technician • ICT co-ordinator • secretary/administrator.	You can have one or more administrators. You may wish to centralise this role or require anyone involved in movement or change of configuration items to be responsible for their own CMDB administration. It is vital that responsibility for updating the CMDB is clear to make sure that it is kept up to date.
Configuration manager	Person with overall responsibility for Configuration Management or ICT in general, eg: • ICT manager • ICT co-ordinator • network manager • technician.	This may be delegated to someone in the ICT team but there should be only one configuration manager for the sake of accountability.
Implementer	Person responsible for carrying out technical changes, eg: • technician • ICT co-ordinator • network manager • supplier • teacher.	Anyone who is authorised to effect changes to the configuration is an implementer by default.

CoM 3.3 Implement

This section tells you how to define and create a configuration management database and populate it with configuration items.

It also describes the methods of keeping the CMDB up to date, which is critical to configuration management. Some of these methods belong to other FITS processes and there will be a link to each one as it is raised in this process.

Step 1: Define configuration item level

Step 2: Define attributes

Step 3: Create CMDB

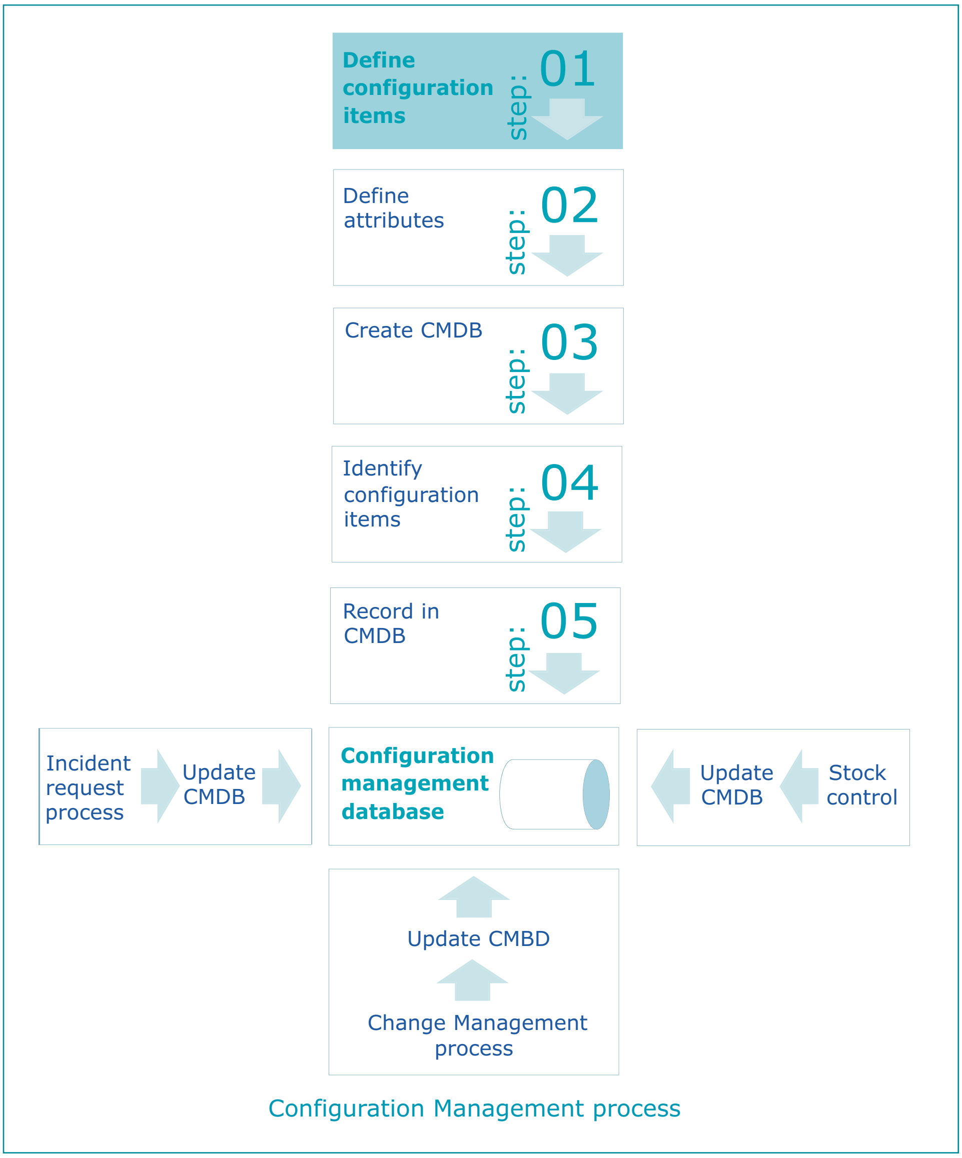
Step 4: Methods of updating CMDB

Step 5: Gather configuration item information

Step 6: Populate CMDB

Step 7: Maintain CMDB

Step 1 Define configuration item level



Configuration Management process

First define the configuration item level at which information is recorded. The more detailed the configuration item level, the more effort is required to maintain it. When beginning the implementation of Configuration Management, it is advisable to keep the configuration item levels high and simple. We have prepared a table of suggested configuration items (see below) to help you with this.

Remember to balance the usefulness of the data against the effort required to gather and maintain it. It may be interesting and valuable to know exactly how many mice there are in school, and to track down where they disappear from. However, it may be more costly in terms of time and effort to do this when compared to the cost of buying a bulk batch of mice every term. Select high-value configuration items to manage first.

Further information about configuration items can be found in CoM 2.4.1Configuration management database.

Suggested configuration items

We recommend that you restrict your configuration items as follows in the first instance:

Configuration item	Components of configuration item
Desktop computer	Peripherals (the mouse, keyboard and monitor are automatically grouped together with the base unit although explicit details of these peripherals are not recorded). Bundled software and licences (such as Microsoft Windows and Microsoft Office) are not recorded separately either.
Laptop computer	Including peripherals and bundled software and licences
File server	Including peripherals and bundled software and licences
Printer	
Router	
Hub/switch	
Communications link	eg ISDN, ADSL, broadband
Software licence	
Manual	Commercial or produced in-house
Procedure	

If you have them, you can add other high-value items, such as a video-conferencing suite or interactive whiteboard, at a similar level.

Step 2 Define attributes

Attributes are the pieces of information recorded against each configuration item. The more attributes you have, the more effort is required to keep them up to date. When beginning the implementation of configuration management it is advisable to keep the list of attributes to a core minimum of information about each configuration item. We have prepared a table of suggested attributes (see below) to help you with this.

Remember to balance maintenance with need. It may be useful to know the name of the supplier and their contact details along with the expiry date of the warranty, but it may be less onerous to record contact information once only and it is likely that the supplier will be able to tell you when the warranty expires. Recording this information explicitly against each configuration item may be heavy handed if you only have two suppliers and their names and numbers are on your telephone list. Select the most useful information to start with: what the item is and where it is.

Further information about attributes can be found in CoM 2.4.1 Configuration management database.

Suggested attributes

We recommend that in the first instance you restrict attributes as follows:

Unique identifier	An assigned number rather than the serial number eg an asset tag, barcode or unique number or reference marked indelibly
Manufacturer	eg Hewlett Packard
Description	eg LaserJet
Assigned to (item)	For use when assigning one item to another eg a software licence to a computer
Assigned to (Person)	For use when assigning an item to an individual or department as opposed to a fixed location eg a laptop to a teacher or student
Location	This can be one or more fields depending on your school eg room and building or, if there is only one building, just room
Date recorded	Date the item was first entered in the CMDB
Date last updated	Date the CMDB record was last changed

Step 3 Create CMDB

We have created a basic configuration management database template (see Appendix C) for you to download and populate. This is based on our suggested configuration items and attributes, but you may add to it as you see fit.

We have also created a configuration management database example (see also Appendix C) to help you understand the content that is required.

Step 4 Implement methods of updating the CMDB

The methods of updating the CMDB need to be in place before you start to gather data and populate the database. This is to ensure that the mechanisms are in place and working to enable updates to be processed as soon as the database is live.

If you audit your equipment and populate your database first, there will be a delay while you implement the update processes. During this time your database will become out of date and you will have to do another audit before you can continue.

There are three channels for updating the configuration management database:

- Request for change process (ChM 3 Change Management Implementation guide)
- Service desk guide to completing the incident/request sheet (Appendix D)
- Stock control (see below).

Stock control

Stock control is needed where configuration items are purchased and held in reserve until they are issued for use. It is important, for asset management and security reasons, to capture and record their details as soon as they are delivered.

A simple 'goods in' stock-control mechanism could be to use the delivery note accompanying the equipment to create new records in the configuration management database as soon as possible after delivery. To do this, make sure that your delivery notes are passed immediately to the CMDB administrator with full attribute information as recorded at 'goods in', such as the location of the equipment following delivery.

'Goods out' should be managed via the request for change or incident/request process.

We have created a goods-in template (Appendix E) for recording configuration items and attribute information at 'goods in' that you may use directly or adapt to suit your environment.

Step 5 Gather configuration item information

Before you gather the configuration item information, you need to define configuration item level (Step 1), define attributes (Step 2) and create the CMDB (Step 3).

Once these have been defined and are in place, you can gather the configuration item information for input. The best way to do this is to carry out a full audit. Bear in mind the following points when carrying out an audit.

- Plan and schedule the audit.
- Freeze the movement of all configuration items to be audited for the duration of the audit.
- Execute the audit quickly, with as little interruption as possible.
- Print out a hard copy of the fields in the database and record data manually in the first instance.
- Alternatively use a laptop to enter data directly into the database.

Step 6 Populate CMDB

When the configuration item data has been gathered, it can be entered into database. Not all the attributes will be appropriate to all configuration items. Where this is the case, enter N/A to show that it is not an omission.

Our attributes example (Appendix B) gives an explanation of each attribute and our example configuration management database (Appendix C) shows you how to apply them.

Step 7 Maintain CMDB

Details of how to maintain the CMDB are described in CoM 4 Operations guide.

CoM 3.4 Review the implementation

After you have created and populated your configuration management database and processed a few changes, ask some key questions and consider the answers before continuing to use the process:

- Did everyone understand what was required of them?
- Was each attribute completed in each configuration item?
- Does training need to be revisited before continuing?
- Are the requests for change, incident/request forms and stock control forms flowing freely to the CMDB administrator?
- Was everyone informed of the new process?

CoM 3.5 Implementation resources

For creating a configuration management database, use the configuration management database template (Appendix C).

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

For creating incident/requests, use the incident/request sheet (Appendix G).

CoM 4 Operations guide

CoM 4.1 What needs to be done?

The ongoing operational tasks for configuration management are:

- updating the configuration management database
- auditing and verifying configuration items
- monitoring the configuration management process
- making decisions.

CoM 4.1.1 Updating the configuration management database

The configuration management database must be continually updated as a result of all additions, moves, removals and changes to configuration items. Failure to do so will result in meaningless information.

Follow the update processes to maintain the database.

- Request for change process (see ChM 3.3 in the FITS Change Management process)
- Service desk guide to completing the incident/request sheet (Appendix D)
- Stock control (see CoM 3.3 Step 4)

CoM 4.1.2 Auditing and verifying configuration items

Periodic checks need to be carried out to ensure that the contents of the configuration management database reflect the reality of the infrastructure. This is done via an audit of all equipment against the records kept. All discrepancies must be noted and the configuration management database brought into line.

Bear in mind the following points when carrying out an audit.

- Plan and schedule the audit.
- Freeze the movement of all configuration items to be audited for the duration of the audit.
- Execute the audit quickly, with as little interruption as possible.
- Print out a hard copy of the fields in the database and record data manually in the first instance.
- Alternatively use a laptop to enter data directly into the database.

CoM 4.1.3 Monitoring the Configuration Management process

It is important to monitor the Configuration Management process to ensure that it is working. The evidence of this will be found during the periodic audit and verification, and the results of this exercise should be published in the form of a report.

The following measurements should be easy to gather and report on:

- number of configuration items in the CMDB at time of audit

- number of physical configuration items following audit
- number of incorrect records in CMDB at time of audit.

To get started on some simple measurements and reporting download our audit report template (see Appendix D) with graphs produced in Excel. Follow the instructions to fill in your volumes of configuration item records, physical items and number of incorrect records and select the graph before printing.

The configuration management audit report example (Appendix D) has been completed with dummy figures.

CoM 4.1.4 Making decisions

The audit report should provide some basic information to help assess the effectiveness of the process. The report itself will not produce the answers, but will provide the starting point for investigation. Remember that there may be many possible reasons for discrepancies – for example:

- more configuration item records than physical items may mean that equipment has been removed without authorisation, or it may mean that equipment has been disposed of legitimately but the records have not been updated
- more physical items than records may mean that new equipment has been implemented but the records not updated, or it may mean that unauthorised equipment has been installed without the knowledge of those responsible for technical support
- an increase in the number of incorrect entries may indicate that the process is not working, or it may be relative to an increased number of requests for change and incident/request forms in that period.

Don't look at the figures in isolation, but consider them within the overall context and also look at the reports from other processes such as Change Management, Incident Management, Problem Management and Release Management.

CoM 4.2 When does it need doing?

Updating the configuration management database

The frequency of updates to the configuration management database will depend on the volume of configuration changes carried out at your particular school.

The important thing to remember is to update the database as soon as possible following a change to ensure that the database is as up to date as possible at all times. It may be more convenient to gather requests for change and incident/request forms into batches for processing, but this will detract from the value of the data you are holding, as it will often be out of date.

Auditing and verifying configuration items

Audit and verification can be time consuming and may therefore be difficult to schedule in a busy environment. However, it is an important part of the process, so allow time for it.

In the early stages of implementation, auditing will need to be more frequent until participants in the process become familiar with it and the tasks become automatic. We recommend that you carry out an audit at the end of the first couple of months after implementation to ensure that there are no issues with the process.

Once the process has become automatic, audits may be less frequent – but this will depend on the individual circumstances of the school and what other factors you may need to consider. For example, new staff may have been trained in the process recently or a new supplier may be involved.

Monitoring the Configuration Management process	The configuration management audit report should be produced after every audit. Regularity is less important than the ability to monitor progress since the previous audit.
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.

CoM 4.3 Who does it?

Updating the configuration management database	The CMDB administrator carries out the updates to the configuration management database. This role may have been allocated to one or more people who receive completed requests for change and incident/request forms at the end of their lifecycle. Alternatively the responsibilities of the CMDB administrator may have been assigned to the main participants in the request for change process and/or the incident/request process. The choice is yours and will depend on your resources.
Auditing and verifying configuration items	The person responsible for ICT or technical support should have the role of configuration manager and is responsible for the auditing of configuration items and their verification against the configuration management database records. This task may be delegated as appropriate.
Monitoring the Configuration Management process	Reporting is the responsibility of the configuration manager (the person responsible for ICT or technical support). However, the configuration manager may delegate it to anyone suitable who has access to audit data.
Making decisions	Decision making in configuration management should be carried out by the person responsible for ICT and/or technical support. 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 in the decision-making process anyone involved in the provision of ICT and technical support.

For further guidance see CoM 3.2.1 Assigning roles and responsibilities in Configuration Management.

CoM 4.4 Operational resources

- Request for change template (Appendix F)
- Incident/request sheet (Appendix G)
- Configuration management audit report template (Appendix D)
- Goods-in template (Appendix E)

CoM 5 Roles and responsibilities

CoM 5.1 CMDB administrator

- Has full access to the configuration management database (CMDB)
- Maintains the configuration management database
- Processes final stage of requests for change and incident/requests
- Has administrative skills
- May be an administrator or a technician

CoM 5.2 Configuration manager

- Is responsible for configuration management
- Is the process owner
- Should have some understanding of the infrastructure
- Does not need to be very technical
- May be the person responsible for ICT and/or technical support
- May be delegated to a technician

CoM 5.3 Implementer

- Implements changes to the configuration
- Deals with incidents and requests
- May also be a CMDB administrator
- Is responsible for following request for change and incident/request processes

CoM 6 Review of Configuration Management

The purpose of this section is to help you review your implementation and ongoing operation of configuration 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 Configuration Management process that you should revisit to make improvements, if these are necessary.

Start by reading the sections included in the recap of Configuration 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.

CoM 6.1 Recap of Configuration Management

In Configuration Management we introduced a method of creating and maintaining a database of records of ICT equipment. We gave you an overview of the whole Configuration Management process and an implementation guide giving step-by-step instructions to help you implement a configuration 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 CoM 6.1.1 to CoM 6.1.4 below.

CoM 6.1.1 Configuration Management summary

Step	Tasks
Create a configuration management database (CMDB)	Peripherals (the mouse, keyboard and monitor are automatically grouped together with the base unit although explicit details of these peripherals are not recorded). Bundled software and licences (such as Microsoft Windows and Microsoft Office) are not recorded separately either.

Step	Tasks
Implement methods of keeping the CMDB up to date	Ensure that the processes used to maintain the CMDB are in place before creating the baseline CMDB, so that you can keep it up to date from the beginning. Keep the CMDB up to date using information gathered in: • change management • incident management • configuration management – stock control. Remember that you need these processes implemented and working properly before you create the CMDB, otherwise you run the risk that the CMDB will become inaccurate because moves and changes are uncontrolled.
Maintain the CMDB	Use information recorded on the forms associated with the update processes (above) to update the CMDB with details of: • changes and moves relating to shared ICT infrastructure equipment, using information from request for change forms • changes and moves relating to end-user ICT equipment, using information from incident/request sheets • the addition of new shared infrastructure or end-user ICT equipment, using information from the goods-in record.
Check that the CMDB and reality are the same	Carry out periodic audits of hardware and software and check the audit findings against the contents of the configuration management database to make sure that everyone is following the update processes.

CoM 6.1.2 What you should expect now that you have implemented Configuration Management

- Technical staff do not move equipment without following the appropriate process to ensure that it is tracked.
- End-users do not move equipment themselves.
- The configuration management database is updated promptly by those responsible for it.
- Access to the configuration management database is controlled.
- Technical support staff carry out regular audits of ICT equipment.
- All ICT equipment has an asset tag.
- New equipment is recorded and tracked as soon as it is delivered.

CoM 6.1.3 What you should have achieved through Configuration Management

- There is a way of keeping a record of all ICT assets.
- The processes for keeping this record up to date have all been implemented (request for change, incident/request, stock control).
- All hardware and software moves and changes are tracked through the update processes.
- Technical support has access to accurate asset records at all times.
- Technical support has access to up-to-date information about ICT equipment.

- There is a way of identifying the age of equipment and planning for its replacement.
- It is possible to account for equipment that has been assigned to departments and individuals.
- The foundation has been laid for technical support to understand the relationships between ICT components.
- An effective CMDB update process means few amendments will need to be made after an ICT audit.

CoM 6.1.4 Benefits of having implemented Configuration Management

- The location of ICT assets is tracked so ICT equipment is less likely to be lost.
- Having a clear picture of what ICT equipment your school already owns helps prevent unnecessary expenditure.
- You will be able to determine the value of ICT assets for the purpose of insurance policies or depreciation calculations.
- You will have accurate hardware information to use in negotiating a price for maintenance contracts – not knowing what needs support is likely to lead to an over-estimation of charges or lack of control of costs.
- Accurate information about equipment helps in planning for changes and upgrades.
- Accurate information about equipment helps in the diagnosis of incidents and problems.
- All information about equipment is in one place, which makes the information easier to maintain and helps it become a trusted source.

CoM 6.2 Checklist

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

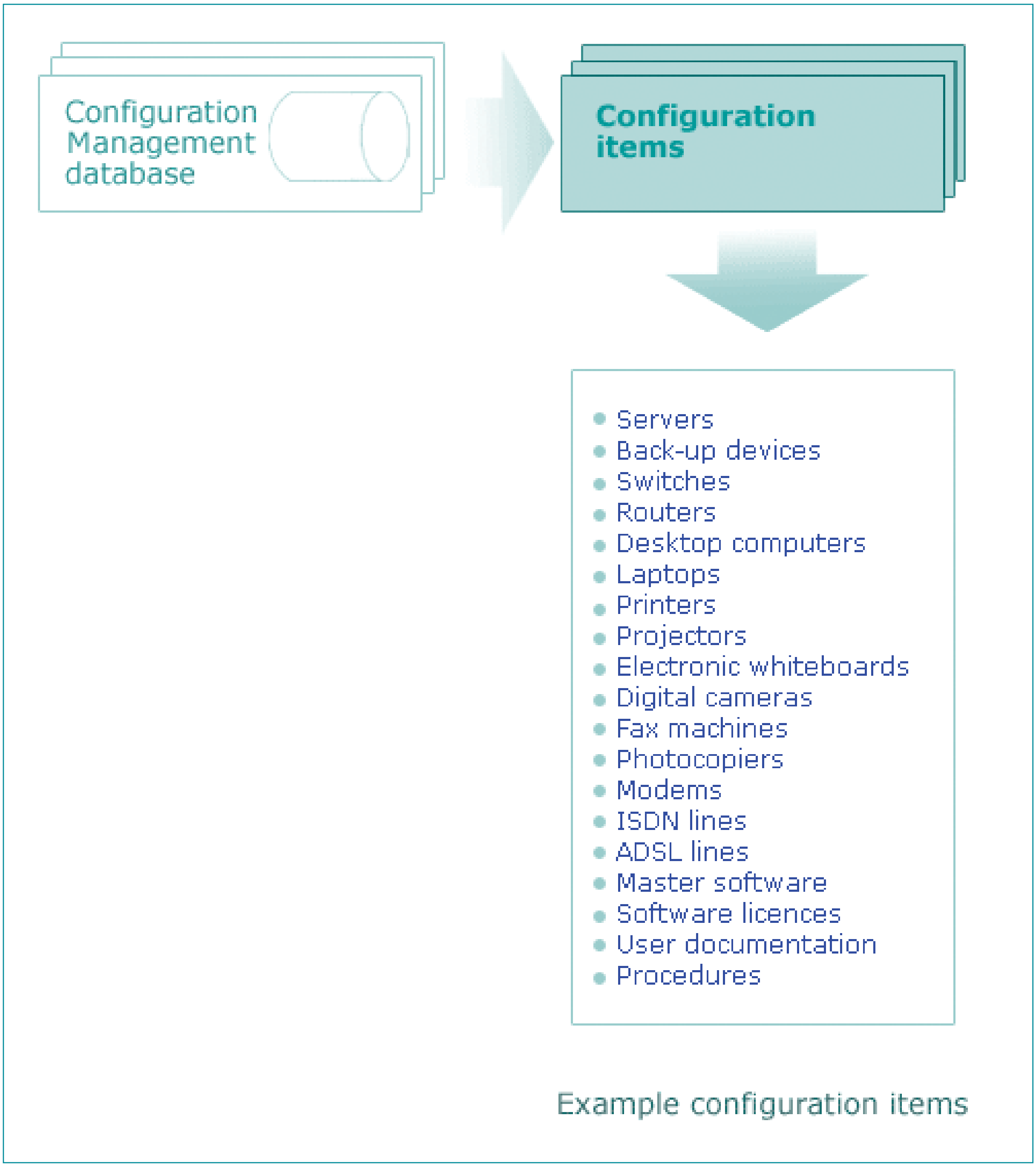
Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful
You have assigned roles and responsibilities.	CoM 3.2.1 Assigning roles and responsibilities in Configuration Management
Participants in the Configuration Management process understand it.	CoM 2 Overview of Configuration Management
You have created a configuration management database (CMDB).	CoM 3 Implement Configuration Management process
The methods for updating the CMDB have been implemented.	CoM 3.3 Step 4 Implement methods of updating CMDB
The CMDB is updated with all hardware and software moves and changes.	CoM 4.1.1 Updating configuration management database CoM 4.2 When does it need doing? CoM 4.3 Who does it?

Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful
Audits of equipment and the CMDB are carried out regularly.	CoM 4.1.2 Auditing and verifying configuration items CoM 4.2 When does it need doing? CoM 4.3 Who does it?
You produce regular configuration management reports.	CoM 4.1.3 Monitoring the Configuration Management process CoM 4.2 When does it need doing? CoM 4.3 Who does it?
You use configuration management reports to understand the use of the process, identify issues and make decisions.	CoM 4.4 Making decisions about Configuration Management CoM 4.2 When does it need doing? CoM 4.3 Who does it?

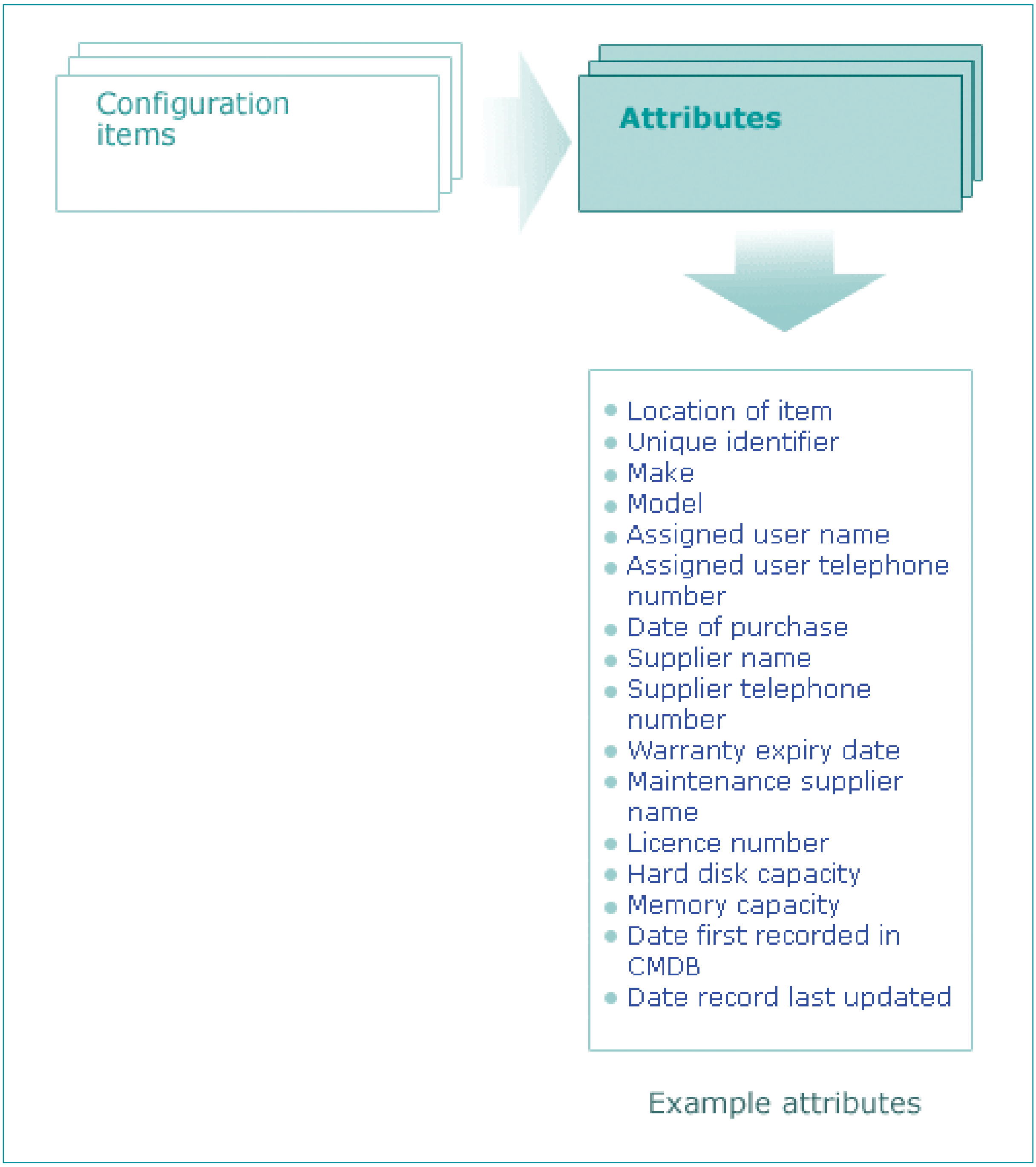
If the above characteristics are all true of your school, congratulations on implementing a successful configuration management process! The next steps for you are to continue operating the process as described in CoM 4 Configuration Management Operations guide and establish the process firmly. Work 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

CoM Appendix A Configuration items – example



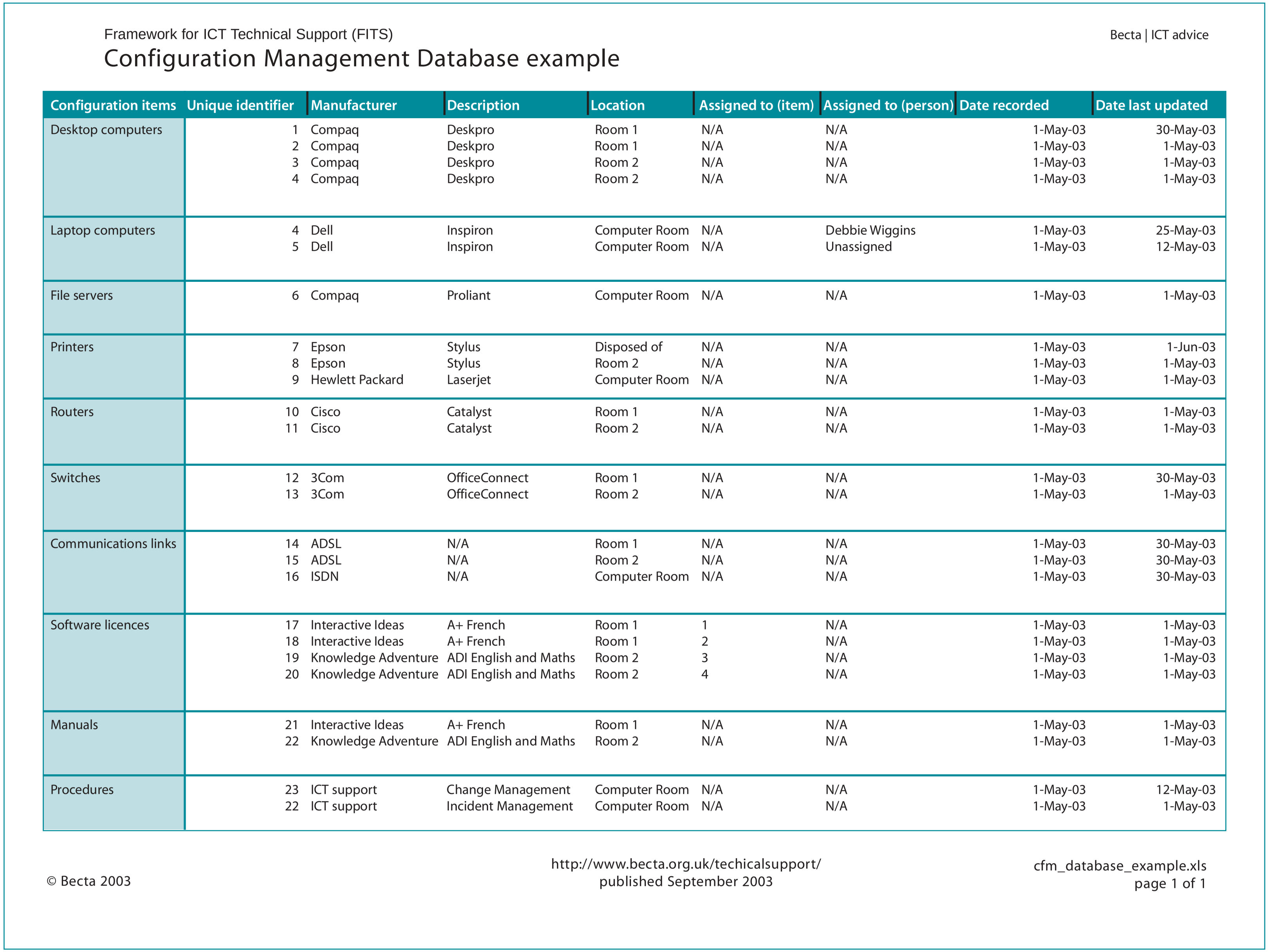
CoM Appendix B Attributes – example



- Location of item
- Unique identifier
- Make
- Model
- Assigned user name
- Assigned user telephone number
- Date of purchase
- Supplier name
- Supplier telephone number
- Warranty expiry date
- Maintenance supplier name
- Licence number
- Hard disk capacity
- Memory capacity
- Date first recorded in CMDB
- Date record last updated

Example attributes

Configuration management database – example and template



Framework for ICT Technical Support (FITS)

Becta | ICT advice

Configuration Management Database example

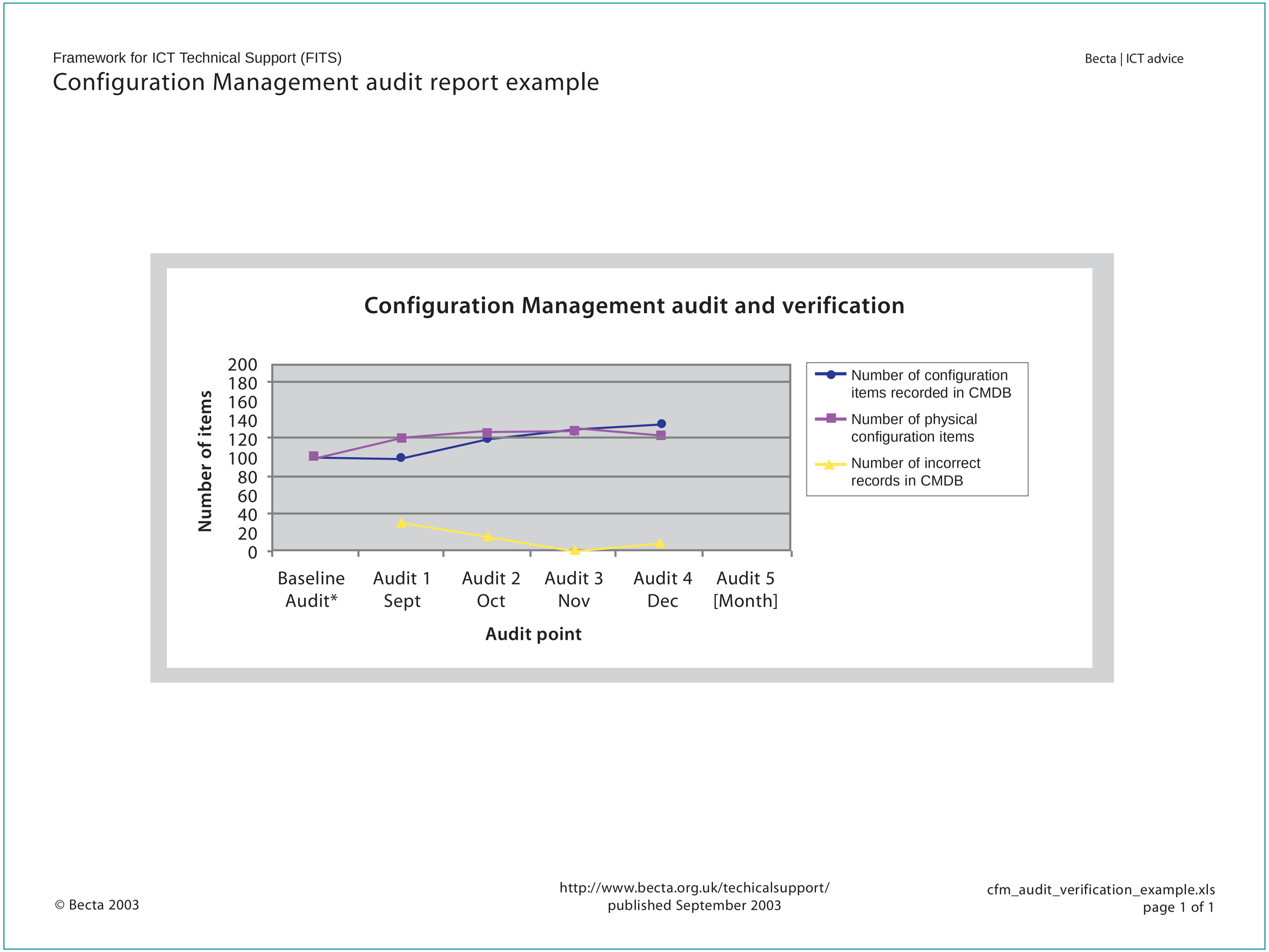
Configuration items	Unique identifier	Manufacturer	Description	Location	Assigned to (item)	Assigned to (person)	Date recorded	Date last updated
Desktop computers	1	Compaq	Deskpro	Room 1	N/A	N/A	1-May-03	30-May-03
	2	Compaq	Deskpro	Room 1	N/A	N/A	1-May-03	1-May-03
	3	Compaq	Deskpro	Room 2	N/A	N/A	1-May-03	1-May-03
	4	Compaq	Deskpro	Room 2	N/A	N/A	1-May-03	1-May-03
Laptop computers	4	Dell	Inspiron	Computer Room	N/A	Debbie Wiggins	1-May-03	25-May-03
	5	Dell	Inspiron	Computer Room	N/A	Unassigned	1-May-03	12-May-03
File servers	6	Compaq	Proliant	Computer Room	N/A	N/A	1-May-03	1-May-03
Printers	7	Epson	Stylus	Disposed of	N/A	N/A	1-May-03	1-Jun-03
	8	Epson	Stylus	Room 2	N/A	N/A	1-May-03	1-May-03
	9	Hewlett Packard	Laserjet	Computer Room	N/A	N/A	1-May-03	1-May-03
Routers	10	Cisco	Catalyst	Room 1	N/A	N/A	1-May-03	1-May-03
	11	Cisco	Catalyst	Room 2	N/A	N/A	1-May-03	1-May-03
Switches	12	3Com	OfficeConnect	Room 1	N/A	N/A	1-May-03	30-May-03
	13	3Com	OfficeConnect	Room 2	N/A	N/A	1-May-03	1-May-03
Communications links	14	ADSL	N/A	Room 1	N/A	N/A	1-May-03	30-May-03
	15	ADSL	N/A	Room 2	N/A	N/A	1-May-03	30-May-03
	16	ISDN	N/A	Computer Room	N/A	N/A	1-May-03	30-May-03
Software licences	17	Interactive Ideas	A+ French	Room 1	1	N/A	1-May-03	1-May-03
	18	Interactive Ideas	A+ French	Room 1	2	N/A	1-May-03	1-May-03
	19	Knowledge Adventure	ADI English and Maths	Room 2	3	N/A	1-May-03	1-May-03
	20	Knowledge Adventure	ADI English and Maths	Room 2	4	N/A	1-May-03	1-May-03
Manuals	21	Interactive Ideas	A+ French	Room 1	N/A	N/A	1-May-03	1-May-03
	22	Knowledge Adventure	ADI English and Maths	Room 2	N/A	N/A	1-May-03	1-May-03
Procedures	23	ICT support	Change Management	Computer Room	N/A	N/A	1-May-03	12-May-03
	22	ICT support	Incident Management	Computer Room	N/A	N/A	1-May-03	1-May-03

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

cfm_database_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=config&id=tt5252

CoM Appendix D Configuration management audit report – example and template



Framework for ICT Technical Support (FITS)

Configuration Management audit report example

Becta | ICT advice

Configuration Management audit and verification

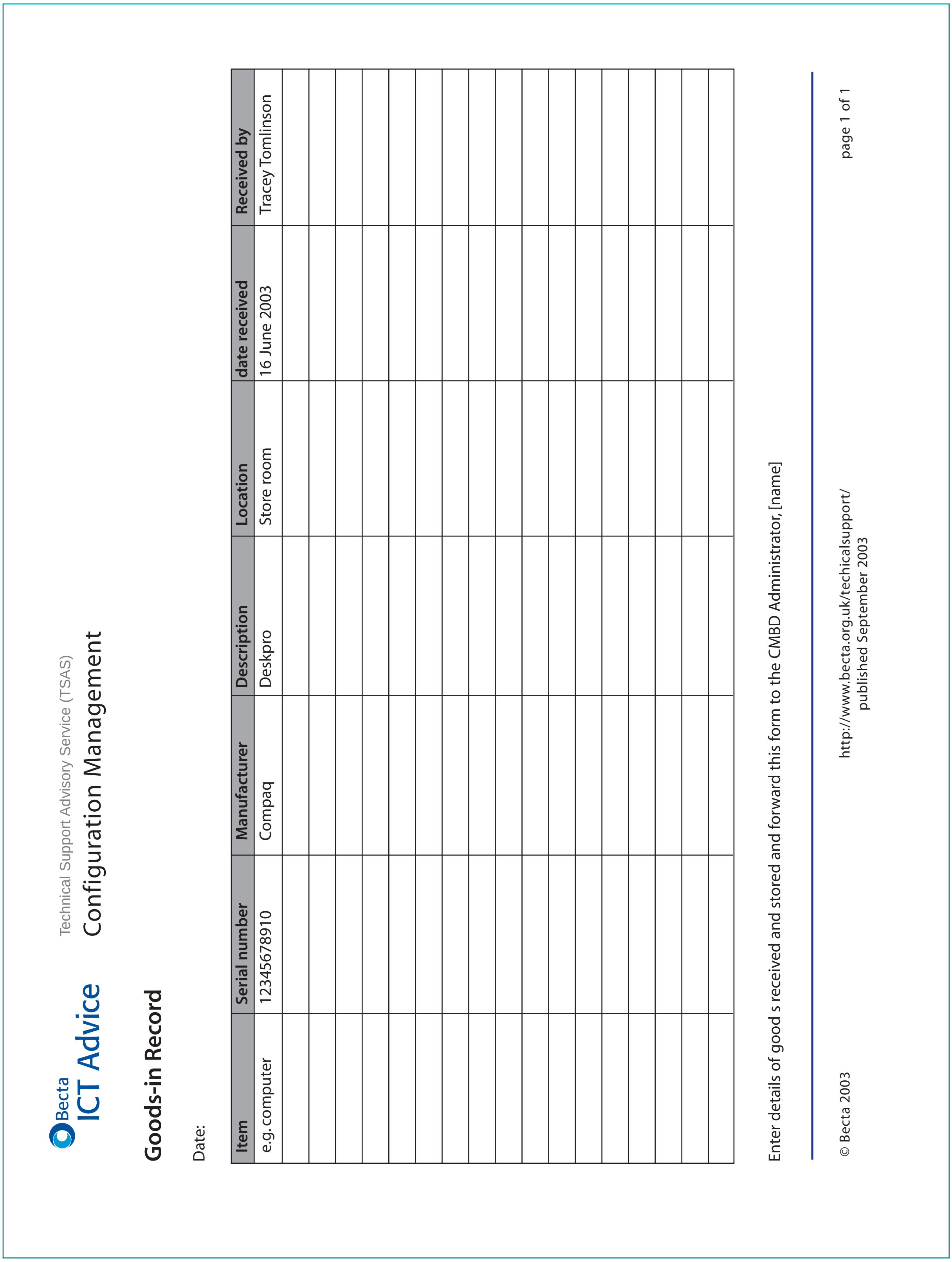
© Becta 2003

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

cfm_audit_verification_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=config&id=tt5252**

CoM Appendix E Goods-in record – template



Becta ICT Advice

Technical Support Advisory Service (TSAS)

Configuration Management

Goods-in Record

Date:

Item	Serial number	Manufacturer	Description	Location	date received	Received by
e.g. computer	12345678910	Compaq	Deskpro	Store room	16 June 2003	Tracey Tomlinson

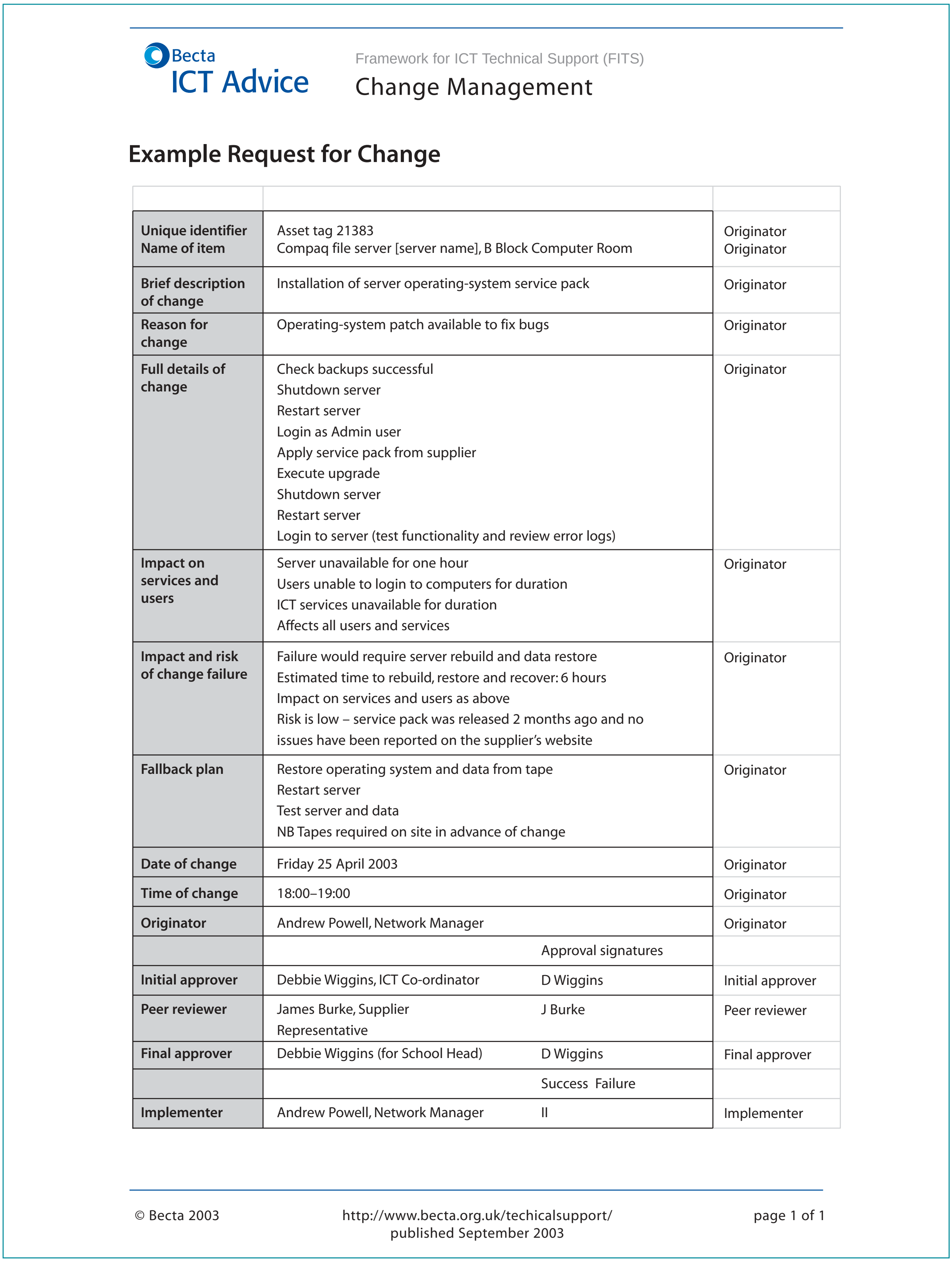
Enter details of good s received and stored and forward this form to the CMBD Administrator, [name]

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

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=config&id=tt5252

CoM Appendix F Request for change – template



Becta ICT Advice

Framework for ICT Technical Support (FITS)

Change Management

Example Request for Change

Unique identifier **Name of item**	Asset tag 21383 Compaq file server [server name], B Block Computer Room		Originator 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	II	Implementer

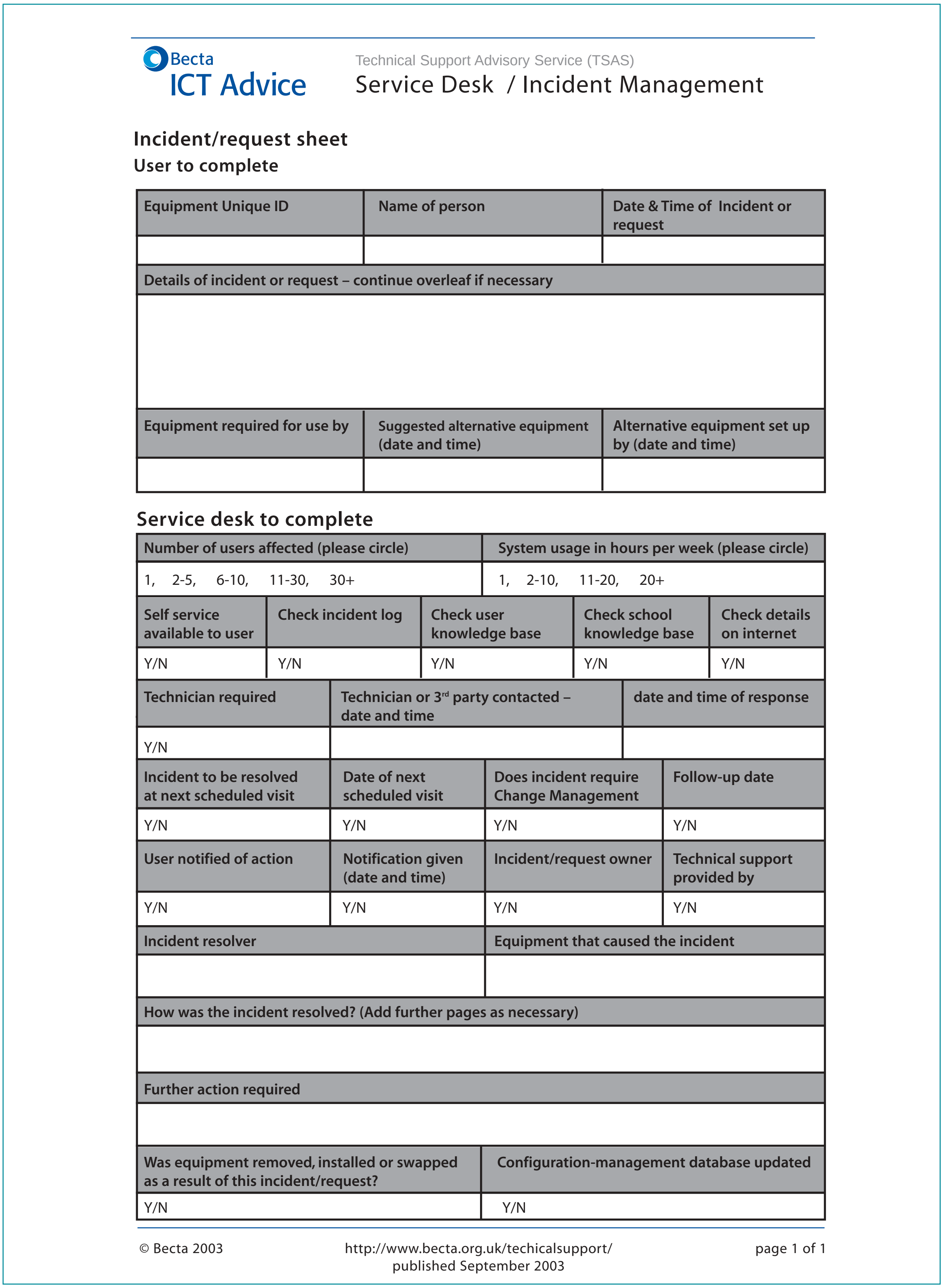
© Becta 2003

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

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**

CoM Appendix G Incident/request sheet



Becta ICT Advice

Technical Support Advisory Service (TSAS)

Service Desk / Incident Management

Incident/request sheet

User to complete

Equipment Unique ID	Name of person	Date & Time of Incident or request
Details of incident or request – continue overleaf if necessary		
Equipment required for use by	Suggested alternative equipment (date and time)	Alternative equipment set up by (date and time)

Service desk to complete

Number of users affected (please circle)	System usage in hours per week (please circle)
1, 2-5, 6-10, 11-30, 30+	1, 2-10, 11-20, 20+

Self service available to user	Check incident log	Check user knowledge base	Check school knowledge base	Check details on internet
Y/N	Y/N	Y/N	Y/N	Y/N

Technician required	Technician or 3rd party contacted – date and time	date and time of response
Y/N		

Incident to be resolved at next scheduled visit	Date of next scheduled visit	Does incident require Change Management	Follow-up date
Y/N	Y/N	Y/N	Y/N
User notified of action	Notification given (date and time)	Incident/request owner	Technical support provided by
Y/N	Y/N	Y/N	Y/N

Incident resolver	Equipment that caused the incident
How was the incident resolved? (Add further pages as necessary)	
Further action required	
Was equipment removed, installed or swapped as a result of this incident/request?	Configuration-management database updated
Y/N	Y/N

© Becta 2003 http://www.becta.org.uk/techicalsupport/ page 1 of 1
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=servdesk&id=dw1039

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).