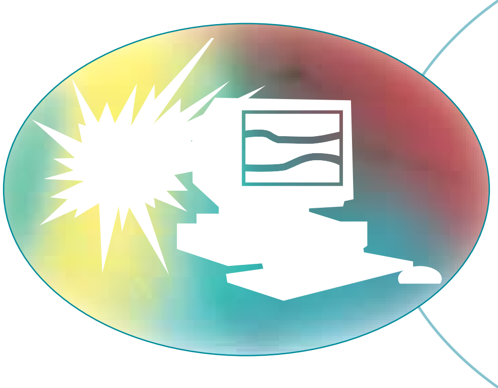


Service Continuity Management

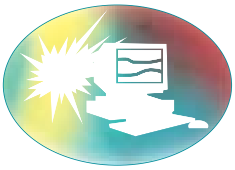
Service Continuity Management Contents

Key

Glossary term:	Glossary term
Cross reference:	Cross reference

Becta
ICT Advice

Framework for ICT Technical Support



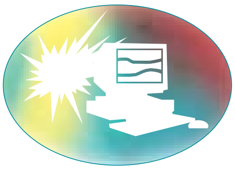
Service Continuity Management

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



Service Continuity Management

SCM 1 Introduction to Service Continuity Management

Do you know which ICT systems are the most critical to your school? If an accident caused them all to fail, would you know where to start to restore the service? Service Continuity Management is what helps you prepare a fallback plan for when the unexpected happens.

SCM 1.1 Aim

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

SCM 1.2 Objectives

The objectives of this section are to enable you to:

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

SCM 2 Overview of Service Continuity Management

SCM 2.1 What is Service Continuity Management?

Service Continuity Management is a reactive and proactive process. It involves contingency planning for recovery in case an unforeseen disaster or event were to seriously affect or destroy ICT service. It also involves risk analysis and the implementation of countermeasures to minimise the likelihood of such an event happening in the first place.

As the title of the process suggests, Service Continuity Management is about maintaining continuity of service – that is to say not just the continuation of equipment (see Appendix A for more information about the difference between services and equipment). It therefore follows that we must consider all components of the service, not just the hardware and software. Similarly, the risks are not confined to the dramatic and remote-sounding examples of fire, flood and terrorist attack. There are many more commonplace possibilities such as a severed cable under a road, a leaking central-heating system, destructive software virus, transport difficulties affecting staff and loss of system password.

SCM 2.2 Why use Service Continuity Management?

The difference between Service Continuity Management and 'disaster recovery' is that Service Continuity Management includes a proactive element to reduce risk, whereas 'disaster recovery' is usually just the reactive part. Other benefits of Service Continuity Management include the following.

- The focus on service, rather than equipment, aligns the process with the overall school and ICT strategy, not just the technical support strategy.
- Having a contingency plan reduces the impact on school activities of a medium- to long-term ICT outage.
- Good service continuity management can help to reduce the cost of insurance.
- It allows technical support to understand the importance and priority of each ICT service within the school, which is beneficial day to day, not just in the event of a disaster.

Don't think 'it won't happen to me'. Service Continuity Management is not just for dramatic disasters – workaday accidents do happen!

SCM 2.3 Who uses Service Continuity Management?

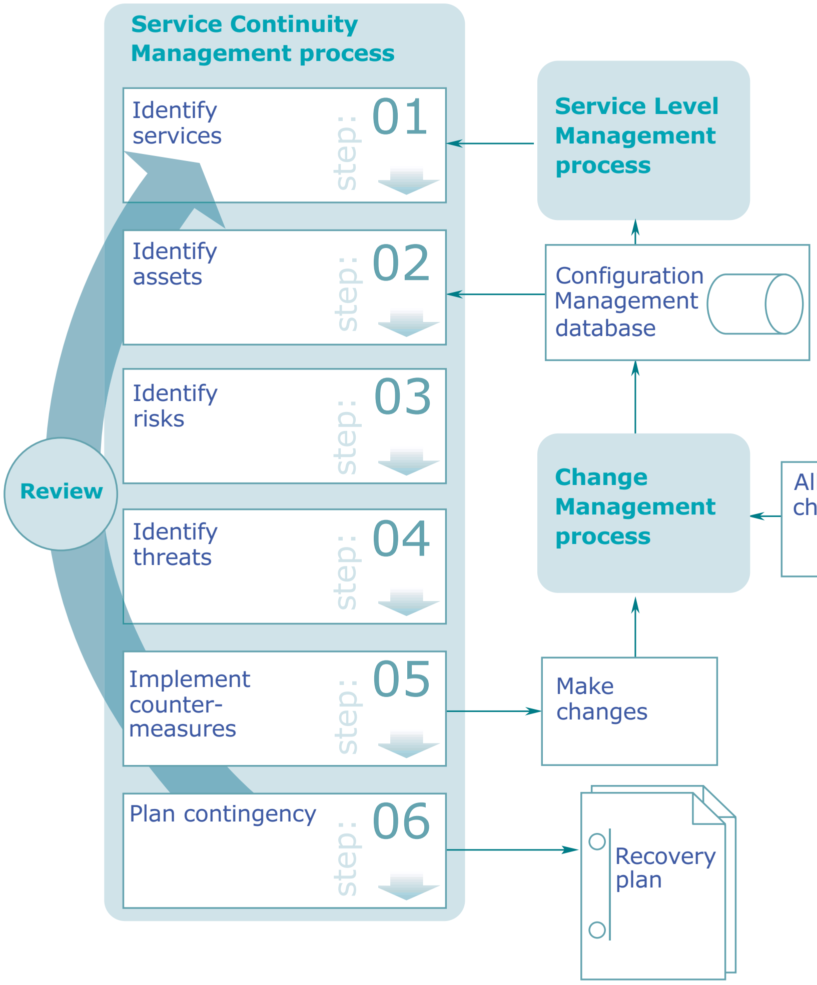
Service Continuity Management in the context of ICT should be initiated and managed by someone with a senior role in ICT or technical support. However, in line with the ICT strategy and because ICT is for the users, it is important that responsibility for service continuity management includes user representatives and authorities such as headteachers. In fact, ICT service continuity management should be part of an overall 'school continuity plan' – after all, recovering the ICT alone will not recreate the school in the event of a disaster.

Remember that third parties such as telecoms providers, support and maintenance suppliers and so on often affect your ICT services. You may therefore need to include them in your discussions and plans because their own service continuity management will have a direct bearing on yours.

SCM 2.4 How Service Continuity Management works

Service Continuity Management works by identifying assets, risks and threats; implementing countermeasures and making contingency plans.

Identify services	Services are the ICT facilities available for users, as opposed to the technical equipment that make up the services (assets). Examples of services are printing, internet access, email and so on.
Identify assets	Assets in this context are IT service components – for example, hardware, software, communication links, buildings, people, procedures, data, contracted suppliers and so on.
Identify risks	Consider what might happen – for example, accidental damage, virus attack, bankruptcy, sickness, sabotage, resignation, power failure and so on.
Identify threats	Consider how likely it is to happen – for example, if access to equipment is uncontrolled, system passwords are common knowledge, building requires maintenance, there are single points of failure and so on.
Implement countermeasures	Reduce the threat as far as possible – for example, tighten security, carry out maintenance, eliminate single points of failure, back up your data and so on.
Plan contingency	Be ready for it to happen anyway: plan and test recovery of service(s).



Service Continuity Management process

Service Continuity Management also interfaces closely with Change Management. As ICT changes, the service continuity requirements also change. It is therefore important that changes are fed into the service continuity plan.

The Service Continuity Management process flowchart (above)illustrates this.

SCM 2.5

What does Service Continuity Management cost?

The cost of Service Continuity Management is very variable. You can spend a little or a lot depending on what you have, what the risks are and what level of risk you consider to be acceptable. The paradox is that you have to incur some cost, even if only in time, in order to find out what the risks might be in the first place.

Expenditure

Money might be spent on reducing risks by buying and implementing technical solutions, such as disk mirroring, back-up systems, uninterruptible power supplies and so on.

Money might be spent on consultancy to carry out the initial risk analysis and/or prepare recovery plans.

Money might be spent on external facilities to aid recovery, such as off-site storage of back-up tapes, off-site availability of spare equipment and so on.

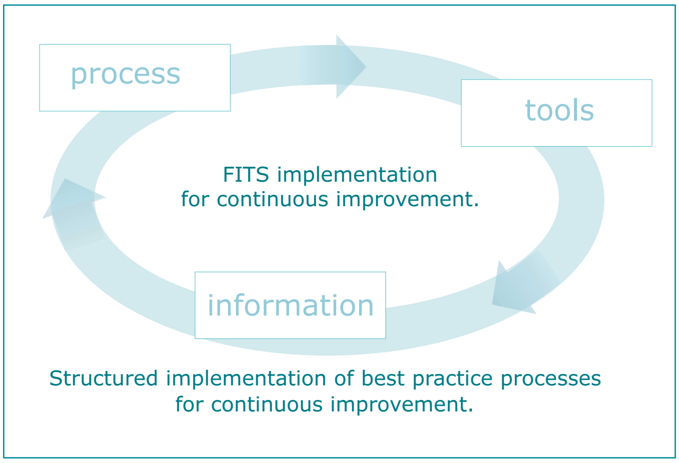
People	People would be needed to manage the process, carry out risk analysis, make any technical changes deemed necessary, develop plans and so on. Recovery plans usually also involve a number of people, including those who would be responsible for initiating and managing the recovery plan, those with technical responsibilities, those with communication responsibilities and so on. These people would need to be involved in the development of the plan and also in testing it.
Time	The amount of time involved will depend on how advanced the school is in implementing processes such as FITS. Some of the work is done in other processes – for instance, identifying services (Service Level Management) and establishing the relationships between infrastructure components (Configuration Management). Also, with good Release Management in place, the planning of new services should help to avoid building in risks.

The cost of Service Continuity Management must be balanced against the value of the ICT service and the potential cost of losing it.

SCM 3 Implementation guide

SCM 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.

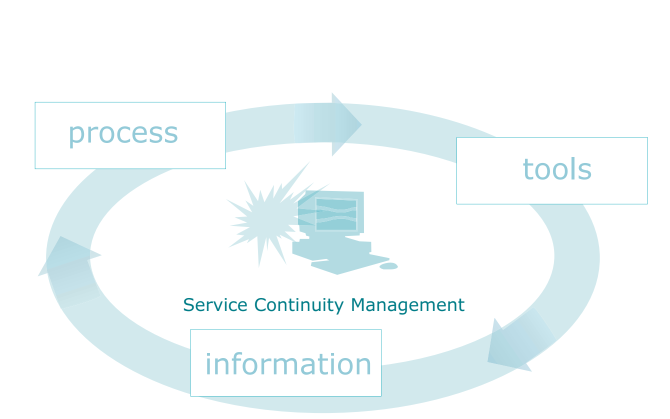

process
tools
FITS implementation
for continuous improvement.
information
Structured implementation of best practice processes
for continuous improvement.

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 Service Continuity 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.



Service Continuity Management implementation approach

Process

Introduce Service Continuity Management process by gathering required data and developing basic contingency and recovery plan

- Identify services and assets
- Identify risks and threats
- Identify countermeasures
- Make and document plans

Tools

Keep tools simple and requiring minimum effort

- Use Word template for recovery plan

Information

Review contingency and recovery plan regularly and feed in new information

- Keep plan up to date
- Improve plan
- Improve countermeasures

SCM 3.1.1 Scope

In introducing service continuity management we do not intend to recommend heavy expenditure or time-consuming tasks. We aim to help you use other FITS processes to become more aware of the needs of service continuity and to improve your ability to respond to a threatening situation.

Service continuity management needs to be ready for any situation. It takes over where preventative maintenance leaves off, in that it is what you need when all else has failed. How serious it is for you depends on how important ICT is to the day-to-day operation of your school. If you can fairly easily and quickly revert to manual procedures or methods, then it is not too much of an issue. If you rely totally on ICT, then it is serious.

The important thing to begin with is that you know what ICT services are used and what the order of criticality is. If you know this, you know where to start and where to finish. You still have to work out how to do it, but at least you know what 'it' is!

The scope of FITS Service Continuity Management, therefore, is to concentrate on defining and prioritising services, identify some potential risks and look at cheap and easy ways in which you can be ready to respond to a major outage.

In the long term, you can examine ways of reducing risks, implement some risk-reducing changes if appropriate, and consider preparing a full contingency plan for your ICT systems. In the short- to medium-term, though, we think that your time would be better spent implementing the other FITS processes to improve the overall resilience and reliability of your ICT infrastructure and minimise some of the risks as you go.

SCM 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

Before you can implement service continuity management, you must assign roles and responsibilities. At this stage we are concerned with what services must be recovered and the order of their recovery, rather than recovery itself. For this reason you need to fulfil only the role of service continuity manager but in SCM 3.2.1 Assigning roles and responsibilities in Service Continuity Management we have included suggestions on fulfilling all roles.

Training	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 part of the training.
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 preparatory tasks before your 'go-live' date.
Communication	Of course, communication must take place within the implementation team, to agree plans, schedule dates and so on. However, 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, prepare 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.
Prerequisites	In some cases you can go straight into implementing a process without having to consider any other dependencies. For Service Continuity Management there are some prerequisites (see SCM 3.2.2).

SCM 3.2.1 Assigning roles and responsibilities in Service Continuity Management

Role	Suggested representative(s)	Comments
Service continuity manager	Person with overall responsibility for ICT/technical support, eg: • ICT manager • ICT co-ordinator • network manager.	The service continuity manager must be abreast of the ICT services in place and what the user priorities are at all times. They should be fully involved in the day-to-day management of ICT and technical support.
Service continuity recovery team	People involved in the service continuity recovery plan, eg • technician(s) • teacher(s) • ICT co-ordinator • classroom assistant(s) • administrator(s) • ICT users.	Membership of the recovery team will vary depending on the severity of the event and the nature of the plan. Members may be involved in setting up and using replacement services on or off site. The team will include technical staff or suppliers whose responsibility it is to restore technical services. Other members of the team will be involved in putting procedures into action and communicating with other school staff (and possibly students). These members may come from anywhere in the school and may be volunteers, in the same sense as fire wardens and first-aid representatives.

SCM 3.2.2 Prerequisites

Service Level Management	Service Level Management requires you to identify services and prioritise them. This can be used as input to the Service Continuity Management process. You should therefore implement Service Level Management as a means to help achieve Service Continuity Management.
Configuration Management	Configuration Management requires you to identify assets (configuration items) and record them in the configuration management database. This data can be used as input to the Service Continuity Management process. You should therefore implement Configuration Management as a means to help achieve Service Continuity Management.
Change Management	Service continuity plans must be changed in line with changes to the ICT in your school. Without a change management process you may not be aware of changes, and your service continuity plans may become out of date and invalid. It is worth while implementing Change Management before Service Continuity Management, but do not let that stop you considering the needs of service continuity management from an early stage. Just being aware of the things to consider may make the difference between success and failure in the event of a disaster.

SCM 3.3 Implement

Service Continuity Management is a process that may evolve over time. Its implementation is not necessarily an end-to-end task that must be finished to have any value. It is something that can be developed over time. It is better to have a vague outline of what to do in the event of a disaster than to have no idea at all.

- Step 1: Identify services and assets
- Step 2: Identify risks and threats
- Step 3: Make contingency plans
- Step 4: Document your recovery plan

Step 1 Identify services and assets

Know what your services and assets are. Assets are the main components of services.

Service	Assets
Printing	Printer
Word processing	Computer, software
Internet	Computer, software, LAN/WAN, communications link, contract with internet service provider (ISP)
Shared data storage	File server, hard disk, software, LAN/WAN
Technical support	Procedures, staff, third-party maintenance contract

Most of this information is gathered in other FITS processes.

- Implement FITS Service Level Management to understand what your services are and what the order of criticality is.

- Implement FITS Configuration Management to get a picture of what your main assets are.

Service continuity also encompasses the human element of ICT by taking into account the continuity of skills, so you will need to add to the above some understanding of the contribution that ICT and user staff make to the success of ICT services. A Becta project called 'ICT Technical Support Training and Accreditation' aims to help schools to assess and develop their technical skills and competencies. Watch the Becta website [**http://www.becta.org.uk**] for new developments and launch details.

Step 2 Identify risks and threats

Before you can know what the risks and threats are to your ICT services and assets, you must first identify services and assets (Step 1). When you have done this, you must consider what might happen to them (risks) and what could cause them to happen (threats). Here is a core list, but you may want to add to it.

Risks	Threats
Loss of internal ICT services and/or assets	Fire, flood, vandalism, weather damage, power failure, power surge, virus, accidental damage, environmental damage
Loss of external ICT services	All of the above, overload of external communications links, bankruptcy
Loss of data	Technical failure, virus, accidental damage, human error
Unavailability of key technical and support staff	Sickness/injury, transport problems, resignation, denial of access to premises
Failure of service providers	Bankruptcy, unavailability of key staff, failure to meet contractual service levels, loss of service provider's own systems or data

Step 3 Make contingency plans

Contingency plans are like insurance policies. They can be simple and cheap but cover you for minimal risk, or they can be complex and expensive and cover you for more risk. As with insurance policies, it all comes down to the level of risk you are taking and the threat of that risk actually happening. It is a judgement decision that you make based on what you know.

If you think it is necessary and worth the expenditure, your contingency plan can be all encompassing and very fast to invoke and implement. For example, you might have a spare set of all hardware, software and back-up data in a workable space offsite, set up and ready to use, or you might buy into a commercial scheme that provides this. Obviously this would not be cheap. Whether you choose to do it or not depends on the potential cost of the loss in the long term and whether or not you think it is worth the risk.

At this stage, you should be starting to think about contingency plans. To help you, we have compiled a list of suggestions for contingency plans that cost little, if any, money. Remember that something is better than nothing, however small.

Suggestions for contingency plans	
Prioritise	Now that you know what your ICT services are and what the order of criticality is, draw up a 'pecking order' of which services to restore first. This will help you prioritise your efforts and make best use of limited contingency facilities.
Reciprocal arrangements	Work with another school or schools to agree a mutual plan to use each other's equipment and premises in the event of a major failure or disaster that prevents access to your own premises. You won't be able simply to transfer everyone from your school to another school, because there won't be enough space, so you will need to scope your requirements and agree what can be done. Use your 'pecking order' of priorities to decide what is essential to start with. When you have done this, you will need to document the plan and make sure that key staff in both schools are aware of it.
Store back-up tapes off site	Agree a mutual arrangement with another school or your LEA to store regular back-up tapes on their premises so that you can access them if your on-site store is damaged.
Share spares	Purchase a spare file server jointly with other schools in your area. This would need careful consideration to make sure that the server was suitable for all schools in the syndicate. You would also need to arrange for it to be stored by a third party (perhaps the supplier).
Store copies of key documentation off site	Make sure that you can access procedures, copies of software licences and key contact information (teachers, suppliers and so on). Make a couple of folders and store them separately. Keep one at home (if this is appropriate) or make a mutual arrangement with another school or a supplier, or give one to a colleague to store off site.
Document manual systems	If you can resort to the manual methods you used before ICT, make sure instructions are documented for quick implementation. This may include use of fax machines instead of email or making sure that learning materials are also available in printed form (and stored off site).

Step 4 Document your recovery plan

We don’t expect you to suddenly produce a sophisticated contingency and recovery plan. However, you might be starting to consider who the key people are and what services you would want to recover first, or be in a position to open discussions with another school about reciprocal arrangements. Don’t put off documenting your thoughts until you have time to prepare your plan all at once: write things down as you go along. In an emergency even just a list of key contacts and telephone numbers would be better than nothing.

Circulate your draft plan to key staff and keep them updated with changes as it develops. You should at least include the headteacher in this. A copy should also be given to anyone on the recovery team. Of course, it is vital that a copy of this document is stored offsite so that you can access it even if you cannot get into the school building.

We have prepared a simple service continuity recovery plan template (see Appendix B) for you to use as a starting point to record the basic information that you may require. See also the service continuity recovery plan example (Appendix B).

SCM 3.4 Review the implementation

A service continuity contingency and recovery plan is bound to change constantly if it is to remain in line with the changes in technology in use and the changing priorities of the school. Once you have started to make contingency and recovery plans, you must review them frequently both to enhance them and also to make sure that they are up to date.

A good way of reviewing what you have done is to rehearse it.

- Invent a scenario that would cause the invocation of the recovery plan and pretend that it has happened.
- Involve the whole recovery team (if you have one at this stage).
- Go through the steps on the recovery plan.
- Ask for feedback from the recovery team afterwards.
- Note any confusion or delay that occurs, so that you can improve the plan.
- Carry out a further role-play: project into the future and imagine what day-to-day ICT functions would be required urgently. Do the priorities in the recovery plan need to change? Is anything missing?

SCM 3.5 Implementation resources

- Service continuity recovery plan template (see Appendix B)
- Service catalogue example and template (Appendix C)
  (See Service Level Management Implementation guide (SLM 3) for full details of how to use this.)
- Configuration management database example and template (Appendix D)
  (See Configuration Management Implementation guide (CoM 3) for full details of how to use this.)

SCM 4 Operations guide

SCM 4.1 What needs to be done

Service Continuity Management is a continuous process, not a one-off exercise. You must review your service continuity recovery plan on a regular basis and do the following:

SCM 4.1.1 Keep the plan up to date

Keep your service continuity recovery plan in line with changes to services and assets. This is managed via other FITS processes:

Configuration Management	The configuration management database should always hold the latest asset information. In service continuity management you would need to know if asset details changed. For example, if you have asked a supplier to reserve a standby server off site for you to use in an emergency, that server would need to keep pace with the on-site equipment's technical specification.
Service Level Management	Service catalogues and service level agreements should have up-to-date details of services in use and service levels required. In service continuity management you would need to know if services or service levels changed. For example, if a new service has been introduced that is more critical to day-to-day school operation than any previous service, this might change the priorities of service recovery.

Change Management	Change Management is the process that ensures that other data sources are up to date. For example, the implementation of a file server upgrade would be carried out via the request-for-change process, which would result in the configuration management database being updated.

The success of your recovery plan will depend on how relevant it is when it is invoked. This success will increase if you implement the above FITS processes to help you keep the plan up to date.

You must also consider changes in personnel and any new appointments to the recovery team and the subsequent training and rehearsal that these may generate.

SCM 4.1.2

Improve the plan

In SCM3 Implementation guide we have made only a very basic start on a recovery plan. We recommend doing something rather than nothing, but try to develop your plan as much as possible. Keep reviewing what you have done so far and consider what improvements you can make.

- Have you identified all your services, assets, risks and threats?
- Are your contingency plans adequate?
- Can you improve the plans you have put in place?
- Can you add to your plans?
- Do you need to rehearse your plans, for the first time or again?

SCM 4.1.3

Improve countermeasures

Review your risks and threats and take action to reduce the possibility that they will occur. A good way to do this as a matter of course is to implement the FITS processes, as these are designed to improve the overall stability and quality of your ICT provision.

Process	Some of the benefits to service continuity
Service Desk	A service desk is a good central point of contact and co-ordination. This centralisation may help you to spot a potential threat and eliminate it before it occurs.
Incident Management	Incident Management provides the data that Problem Management uses to identify trends and underlying problems. Without it, Problem Management would not be able to improve resilience and quality of services.
Problem Management	Problem Management is concerned with eliminating underlying problems and identifying trends. This may act as an early-warning system and enable you to improve resilience.
Change Management	As well as being the process that helps to keep the recovery plan up to date, Change Management helps to improve the quality of technical solutions and therefore the resilience.
Configuration Management	Configuration Management is the central point for all data concerning assets (configuration items) and the relationships between them. This helps when planning changes to ensure that you maintain resilience. It also exposes single points of failure that you can eliminate.
Release Management	Release Management is concerned with the planning and implementation of new services. This is where the design of a service is considered and single points of failure removed at source – the ultimate in proactive support.

Availability Management	Availability and Capacity Management is closely tied to Service Continuity Management, as their concepts are similar – keeping services available continuously or as required and ensuring that there is sufficient processing and storage capability. Preventative Maintenance is a key element of risk management and includes equipment health checks and the creation and testing of back-ups, as well as the building in of contingency such as disk mirroring or RAID and eliminating single points of failure. Network Monitoring also provides valuable advance notice of potential availability and capacity problems and helps you to avoid them.
Service Level Management	Service Level Management provides input to Service Continuity Management in the form of details and relative importance of services. The better this process, the better you understand what is required of Service Continuity Management. If you have got as far as drawing up service level agreements with ICT users, you will already have had to consider how you are going to meet the terms of those agreements and provide a consistent service so you have a head start on Service Continuity Management.
Financial Management	Good financial management means that you are spending only what is required on ICT and technical support. Any spare cash could go into service continuity management to improve that further.

SCM 4.2 When does it need doing?

Operational task	Frequency
Keep the plan up to date (SCM 4.1.1)	Whenever there is a significant change to services or equipment
Improve the plan (SCM 4.1.2)	As often as possible – review at least once a year
Improve countermeasures (SCM 4.1.3)	As often as possible – review at least once a year

SCM 4.3 Who does it?

Operational task	Who does it?
Keep the plan up to date (SCM 4.1.1)	Service continuity manager
Improve the plan (SCM 4.1.2)	Service continuity manager
Improve countermeasures (SCM 4.1.3)	Service continuity manager

SCM 4.4 Operational resources

The operational resources for service continuity management are the tools you have developed yourself in this process and others.

- Service continuity recovery plan (Appendix B)
  (See Service Continuity Management Implementation guide (SCM 3) for details of how to create this.)
- Service catalogue (Appendix C)
  (See Service Level Management Implementation guide (SLM 3) for details of how to create this.)
- Configuration management database (Appendix D)
  (See Configuration Management Implementation guide (CoM 3) for details of how to create this.)

SCM 5 Roles and responsibilities

SCM 5.1 Service continuity manager

- Is responsible for service continuity
- Is the service continuity management process owner
- Leads the development of the service continuity recovery plan
- Is the person who invokes the service continuity recovery plan
- Is a senior member of the ICT or technical support staff
- Does not need to be technical
- Must understand the ICT priorities of the users
- Should not delegate responsibility
- Should have cover during absence

SCM 5.2 Service continuity recovery team

- Participates in the testing and invocation of the service continuity recovery plan
- Includes technical staff for technical procedures
- Includes users for testing and during actual invocation
- Includes departmental representatives for communication and co-ordination (in testing and in invocation)
- Is led by the service continuity manager

SCM 6 Review of Service Continuity Management

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

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

SCM 6.1 Recap of Service Continuity Management

In Service Continuity Management we introduced the idea of being prepared to recover ICT services in the event of a disaster and also of being proactive in minimising the likelihood of a disaster affecting ICT services. We gave you an overview of the whole Service Continuity Management process and an implementation guide giving step-by-step instructions to help you implement a service continuity management process and contingency plan 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 SCM 6.1.1 to SCM 6.1.4 below.

SCM 6.1.1 Service Continuity Management summary

Step	Tasks
Identify the ICT services in use so that you understand what would need to be restored and in what order.	Identify and document services. This task is part of Service Level Management.
Identify the components that enable those services so that you understand what equipment would be needed to restore services.	Identify and document equipment. This task is part of Configuration Management.
Identify the risks and threats that may result in a disastrous situation.	Consider all the things that might happen, such as: • fire • flood • accidental damage. • Take into account how likely to happen these are. For example: • a flood is more likely if the school is next to a river that is prone to bursting its banks • accidental damage to a file server may be more likely if it is in a classroom rather than in a secure room of its own.
Implement countermeasures to reduce the risks and threats.	Taking steps to reduce the risks and threats is the proactive part of Service Continuity Management. Taking some of the examples above, your countermeasures might include: • housing as much computer infrastructure equipment as possible on a high floor in the building, to minimise the risk of water damage in the event of a flood • placing the file server out of general reach on a purpose-built rack, to protect it from the comings and goings of the classroom.
Make contingency plans to be invoked in the event of a disaster affecting ICT services.	Draw up a plan to help you restore ICT services. This may include operating a temporary service in alternative accommodation or it may focus entirely on the restoration of the original service in situ. The latter is likely to take longer, depending on the extent of the disaster and factors such as access to the premises and obtaining replacement equipment. The former may be desirable if a speedy restoration is the priority, but you will need additional resources such as access to alternative accommodation and equipment, that you do not need for the recovery of the original service.

SCM 6.1.2 What you expect now that you have implemented Service Continuity Management

- There is an increased awareness of the possibility of the unforeseen occurring.
- There is an increased awareness of the importance and priority of ICT services.
- ICT staff, end-users and suppliers involved in a contingency plan know what is required of them.

- You have given more thought to resilience and the possible risks affecting the availability of ICT services, and you leave less to chance.

SCM 6.1.3 What you should have achieved through Service Continuity Management

- You have created a service catalogue documenting all ICT services in use.
- You have a configuration management database that holds details of all ICT equipment.
- You have prepared a contingency plan that can be invoked in the event of a disaster or accident.
- You have rehearsed the contingency plan with all participants.
- You keep a copy of your contingency plan securely off site as well as one on site.
- You keep the contingency plan up to date with changes to ICT services and user requirements.
- As far as possible, you have neutralised all risks and threats to ICT services.

SCM 6.1.4 Benefits of having implemented Service Continuity Management

- In the event of an accident or disaster, you could restore ICT services in the correct order of importance.
- The readiness of a contingency plan means that you would lose little time in reacting to and recovering from an accident or disaster.
- Projecting a disaster scenario helps people to prepare mentally for such an event.
- An accident or disaster is less likely to happen because you have acknowledged and minimised risks and threats.
- Service continuity and disaster recovery is aligned with the overall needs of the school and ICT strategy, not just the technical support strategy.
- There is a clearer understanding of the importance and rank of ICT services and so better focus of resources day to day, not just in the event of a disaster.

SCM 6.2 Checklist

Use this checklist to identify any areas of service continuity 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.	SCM 3.2.1	Assigning roles and responsibilities in Service Continuity Management
Participants in service continuity management understand the process.	SCM 2	Overview of Service Continuity Management
You have identified and documented ICT services and equipment.	SCM 3.3	Step 1Identify services and assets
Risks and threats to ICT services and equipment have been acknowledged.	SCM 3.3	Step 2 Identify risks and threats
You have drawn up contingency plans.	SCM 3.3	Step 3 Make contingency plans

You have prepared a service continuity recovery plan.	SCM 3.3 Step 4 Document your recovery plan
You update the service continuity recovery plan as changes are made to ICT services.	SCM 4.1.1 Keep the plan up to date SCM 4.2 When does it need doing? SCM 4.3 Who does it?
The service continuity recovery plan is as comprehensive as possible.	SCM 4.1.2 Improve the plan
As far as possible, you have implemented countermeasures to risks and threats.	SCM 4.1.3 Improve countermeasures

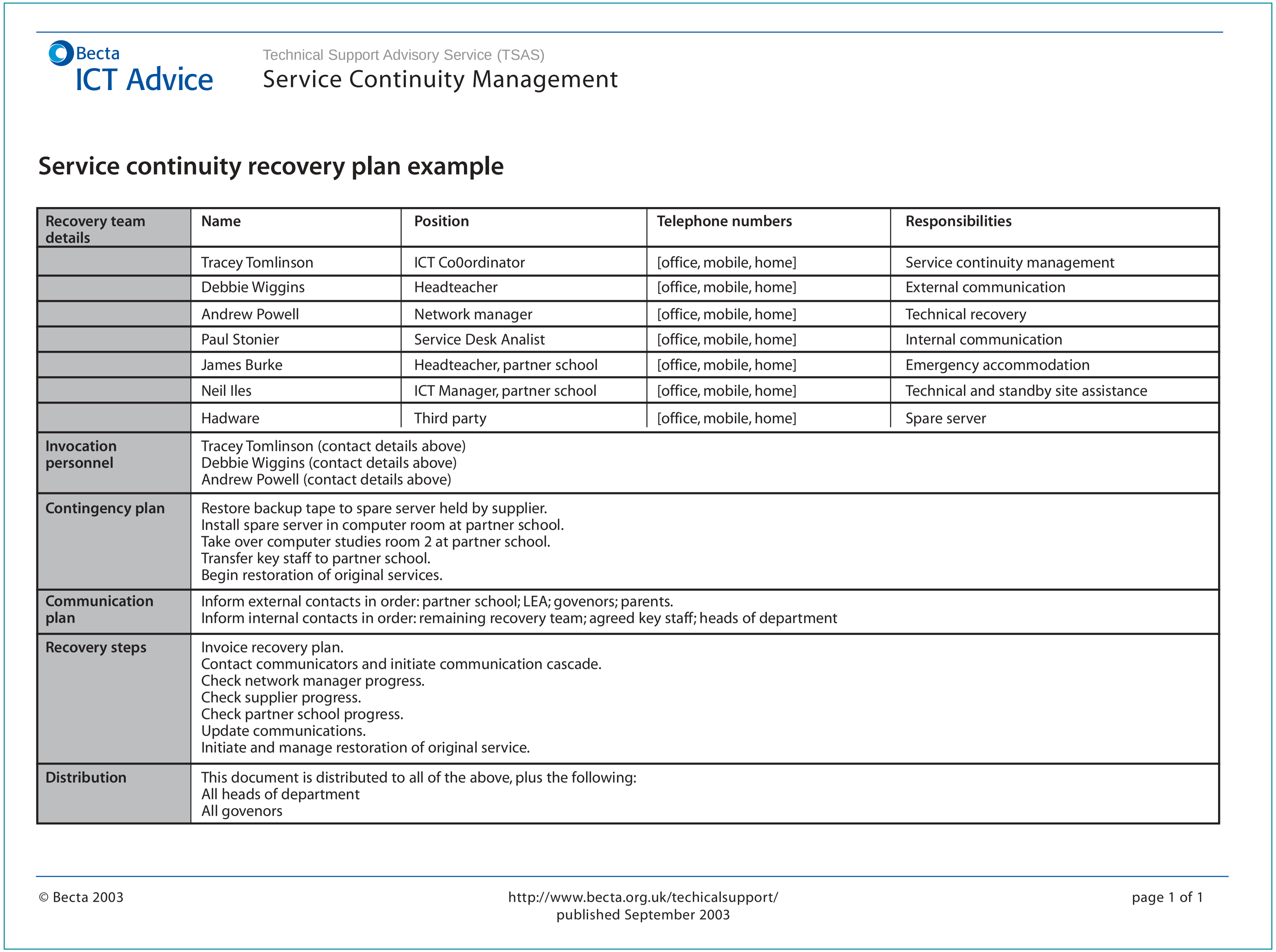
If the above characteristics are all true of your school, congratulations on implementing a successful service continuity management process! The next steps for you are to continue operating the process as described in the Service Continuity Management Operations guide (SCM 4) and establish the process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

Appendices

SCM Appendix A Example services

Service	Equipment required to enable service
Printing	Printer, computer, cable, ink cartridge, paper, printer driver, electrical power
Word processing	Computer, operating system, word processing software, electrical power
Internet access	Computer, operating system, internet-browser software, communications link, internet service provider (ISP), electrical power
Shared data storage	File server, computer, network operating system, computer operating system, routers, switches, hubs, network cabling, communication links, electrical power

SCM Appendix B Service continuity recovery plan – example and template



Becta
ICT Advice

Technical Support Advisory Service (TSAS)
Service Continuity Management

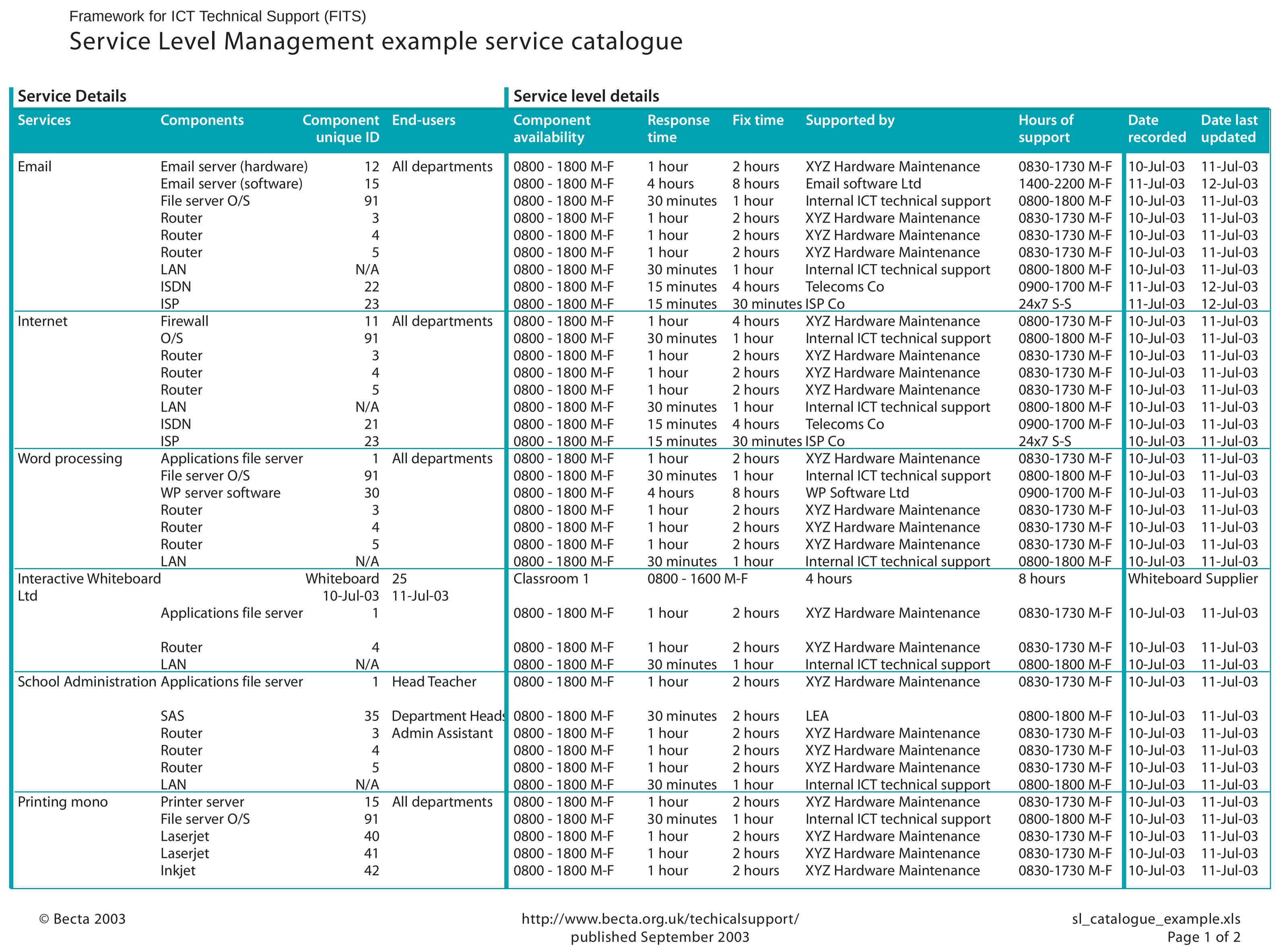
Service continuity recovery plan example

Recovery team details	Name	Position	Telephone numbers	Responsibilities
	Tracey Tomlinson	ICT Co0ordinator	[office, mobile, home]	Service continuity management
	Debbie Wiggins	Headteacher	[office, mobile, home]	External communication
	Andrew Powell	Network manager	[office, mobile, home]	Technical recovery
	Paul Stonier	Service Desk Analist	[office, mobile, home]	Internal communication
	James Burke	Headteacher, partner school	[office, mobile, home]	Emergency accommodation
	Neil Iles	ICT Manager, partner school	[office, mobile, home]	Technical and standby site assistance
	Hadware	Third party	[office, mobile, home]	Spare server
Invocation personnel	Tracey Tomlinson (contact details above) Debbie Wiggins (contact details above) Andrew Powell (contact details above)			
Contingency plan	Restore backup tape to spare server held by supplier. Install spare server in computer room at partner school. Take over computer studies room 2 at partner school. Transfer key staff to partner school. Begin restoration of original services.			
Communication plan	Inform external contacts in order: partner school; LEA; govenors; parents. Inform internal contacts in order: remaining recovery team; agreed key staff; heads of department			
Recovery steps	Invoice recovery plan. Contact communicators and initiate communication cascade. Check network manager progress. Check supplier progress. Check partner school progress. Update communications. Initiate and manage restoration of original service.			
Distribution	This document is distributed to all of the above, plus the following: All heads of department All govenors			

© 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=servcont&id=tt5470

SCM Appendix C Service catalogue – example and template



Framework for ICT Technical Support (FITS)

Service Level Management example service catalogue

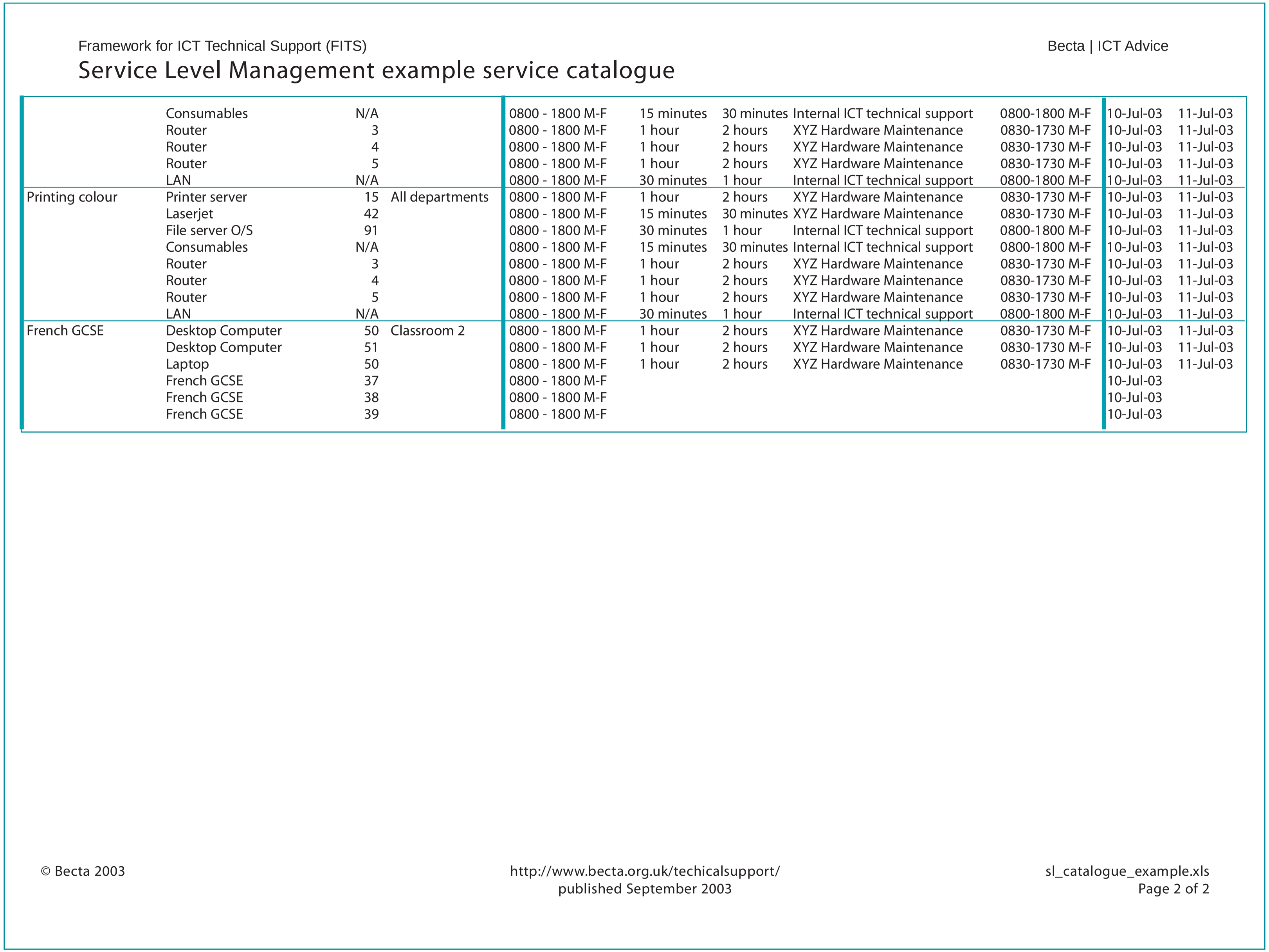
Service Details				Service level details						
Services	Components	Component unique ID	End-users	Component availability	Response time	Fix time	Supported by	Hours of support	Date recorded	Date last updated
Email	Email server (hardware)	12	All departments	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Email server (software)	15		0800 - 1800 M-F	4 hours	8 hours	Email software Ltd	1400-2200 M-F	11-Jul-03	12-Jul-03
	File server O/S	91		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Router	3		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	ISDN	22		0800 - 1800 M-F	15 minutes	4 hours	Telecoms Co	0900-1700 M-F	11-Jul-03	12-Jul-03
	ISP	23		0800 - 1800 M-F	15 minutes	30 minutes	ISP Co	24x7 S-S	11-Jul-03	12-Jul-03
Internet	Firewall	11	All departments	0800 - 1800 M-F	1 hour	4 hours	XYZ Hardware Maintenance	0800-1730 M-F	10-Jul-03	11-Jul-03
	O/S	91		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Router	3		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	ISDN	21		0800 - 1800 M-F	15 minutes	4 hours	Telecoms Co	0900-1700 M-F	10-Jul-03	11-Jul-03
	ISP	23		0800 - 1800 M-F	15 minutes	30 minutes	ISP Co	24x7 S-S	10-Jul-03	11-Jul-03
Word processing	Applications file server	1	All departments	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	File server O/S	91		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	WP server software	30		0800 - 1800 M-F	4 hours	8 hours	WP Software Ltd	0900-1700 M-F	10-Jul-03	11-Jul-03
	Router	3		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
Interactive Whiteboard Ltd		Whiteboard 10-Jul-03	25 11-Jul-03	Classroom 1	0800 - 1600 M-F		4 hours	8 hours	Whiteboard Supplier	
	Applications file server	1		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
School Administration	Applications file server	1	Head Teacher	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	SAS	35	Department Heads	0800 - 1800 M-F	30 minutes	2 hours	LEA	0800-1800 M-F	10-Jul-03	11-Jul-03
	Router	3	Admin Assistant	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
Printing mono	Printer server	15	All departments	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	File server O/S	91		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Laserjet	40		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Laserjet	41		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Inkjet	42		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03

© Becta 2003

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

sl_catalogue_example.xls
Page 1 of 2

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=servlevel&id=tt5367



Framework for ICT Technical Support (FITS)

Becta | ICT Advice

Service Level Management example service catalogue

	Consumables	N/A		0800 - 1800 M-F	15 minutes	30 minutes	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Router	3		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
Printing colour	Printer server	15	All departments	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Laserjet	42		0800 - 1800 M-F	15 minutes	30 minutes	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	File server O/S	91		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Consumables	N/A		0800 - 1800 M-F	15 minutes	30 minutes	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
	Router	3		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	4		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Router	5		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	LAN	N/A		0800 - 1800 M-F	30 minutes	1 hour	Internal ICT technical support	0800-1800 M-F	10-Jul-03	11-Jul-03
French GCSE	Desktop Computer	50	Classroom 2	0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Desktop Computer	51		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	Laptop	50		0800 - 1800 M-F	1 hour	2 hours	XYZ Hardware Maintenance	0830-1730 M-F	10-Jul-03	11-Jul-03
	French GCSE	37		0800 - 1800 M-F					10-Jul-03	
	French GCSE	38		0800 - 1800 M-F					10-Jul-03	
	French GCSE	39		0800 - 1800 M-F					10-Jul-03	

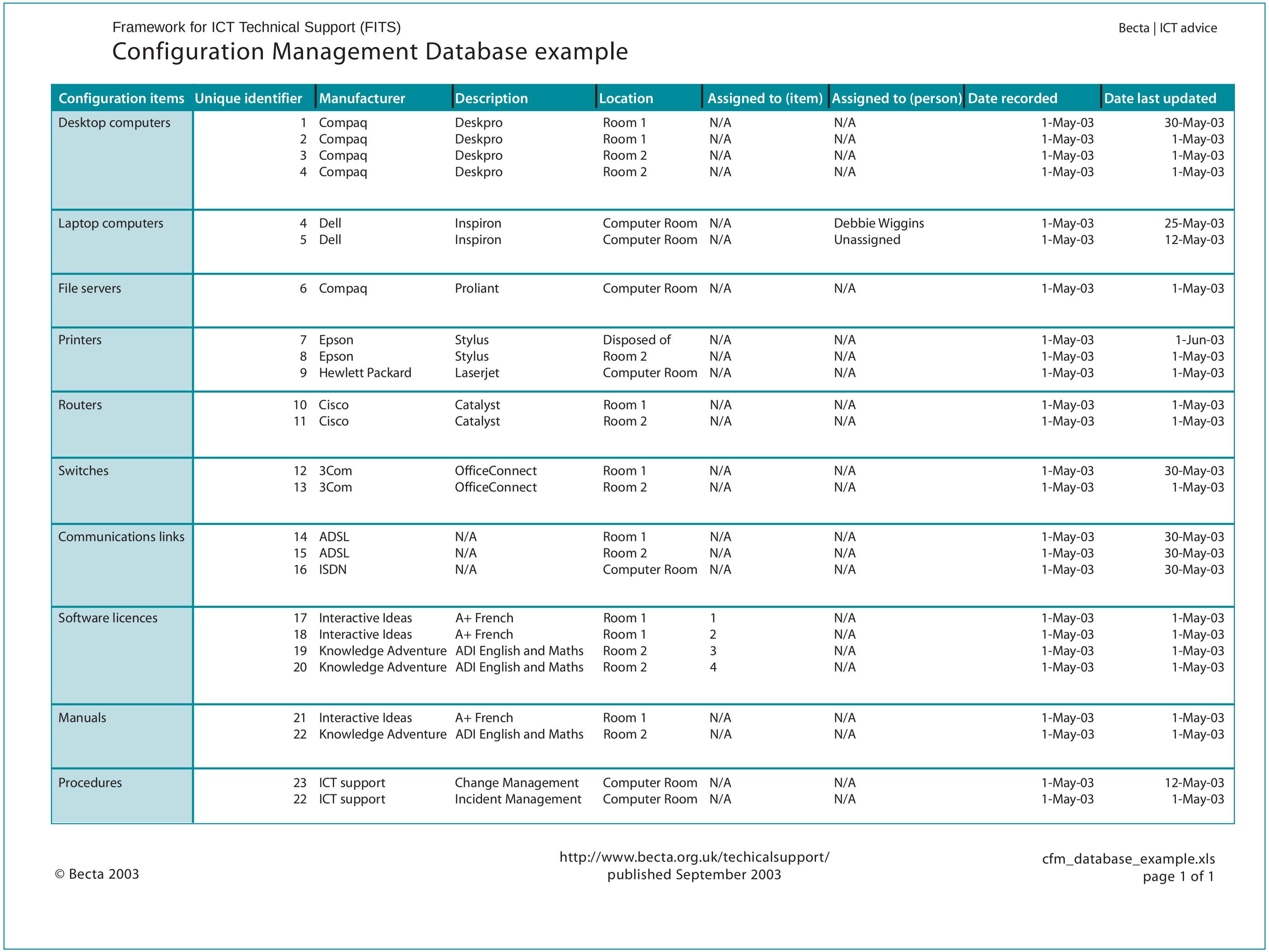
© Becta 2003

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

sl_catalogue_example.xls
Page 2 of 2

You can download the template from the FITS website
http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=servlevel&id=tt5367

SCM Appendix D 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**

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).