



## About this guide

This pocket guide is designed as a handy reference book for anyone involved in ICT management or day-to-day technical support in schools. It can also be used by anyone defining ICT or technical support strategy in schools. The guide is complementary to the Framework for ICT Technical Support (FITS), developed by Becta and freely available on the Becta website.

**<http://www.becta.org.uk/leaders/technicalsupport>**

In this guide we explain the processes of FITS, which cover the four main functions of technical support provision:

- Reactive
- Proactive
- Change
- Strategic.

Based on FITS best practice, the advice given within this set of guidelines is neither definitive nor prescriptive. It is of benefit and applicable to all schools irrespective of size or the technology in use. The guidelines should be adapted and adopted to fit each school individually, based on the school's resources and needs.

The key message we want to reinforce is that ICT services are there solely to support the school and its efficient and effective operation.



## Contents

Introduction to FITS	3
Processes of FITS	4
Where to start	5
Roles and resources	6
Technical support strategy	7
Measuring the performance of technical support	8
Tools for technical support	8
Service Desk	10
Incident Management	14
Problem Management	18
Change Management	22
Release Management	26
Configuration Management	30
Availability and Capacity Management	34
Preventative Maintenance	36
Network Monitoring	39
Service Level Management	42
Service Continuity Management	46
Financial Management	50
Further guidance and contact points	54

## Introduction to FITS

FITS stands for Framework for ICT Technical Support and is based on the IT Infrastructure Library (ITIL).

ITIL is derived from the collective experiences of ICT technical support providers all over the UK. It represents their learning curve over the last 20 years and has been distilled into a set of common processes applicable to any establishment using ICT. FITS is designed to enable you to implement the processes successfully and avoid all the mistakes commonly made. The emphasis is on proactive tasks as well as reactive ones. Technical support is not just a function responsible for resolving incidents, but a service provider whose main objective is incident prevention. We see this as the ultimate goal of technical support and aim to help you make it happen.

Here are just a few of the many benefits FITS offers:

- the benefit of 20+ years' experience of developing ICT technical support techniques
- tried and tested processes, adapted with the school environment in mind
- simplified processes ready for immediate use
- templates, checklists and downloads that can be used as they are or personalised
- a quick-start approach to help you make the best use of time and resources and see quick results
- separated administrative and technical tasks to help you assign the most appropriate resources
- help in keeping costs to a minimum
- help to protect teachers from getting too involved in technical support issues
- help in measuring technical support.

## Processes of FITS

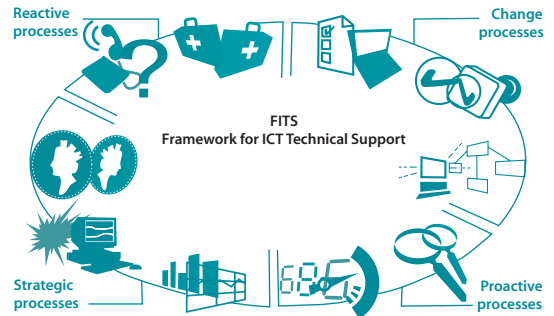
FITS has 10 main process topics, each covering a different area of best-practice technical support.

---

	Service Desk
	Incident Management
	Problem Management
	Change Management
	Release Management
	Configuration Management
	Availability and Capacity Management
	Service Level Management
	Service Continuity Management
	Financial Management

---

We have grouped the processes together under four headings, to illustrate the nature of each process and where they fit into the lifecycle of technical support.



FITS' processes match in name and definition the processes of the IT Infrastructure Library. We have adapted the processes themselves to form a manageable and relevant set of procedures that are ready to be implemented in schools.

### Where to start

It should be possible to begin by implementing any process. However, depending upon the maturity of your ICT and technical support, there are appropriate places to start to maximise the chance of success.

The recommended path for established technical support and/or ICT functions is:

- ▼ Service Desk
- ▼ Incident Management
- ▼ Change Management
- ▼ Availability and Capacity Management:  
Network Monitoring
- ▼ Configuration Management
- ▼ Availability and Capacity Management:  
Preventative Maintenance
- ▼ Release Management
- ▼ Problem Management
- ▼ Service Level Management
- ▼ Service Continuity Management
- ▼ Financial Management

## Roles and resources

When planning to implement processes, you will need to consider the role requirements and the resources available to you. These may include:

- suppliers
- ICT or technical support staff
- teaching staff
- school administrative staff
- contractors
- other school staff
- technical staff from other schools.

It is important to consider your resources carefully to ensure best fit of people skills with process roles and requirements. When assigning roles to individuals, consider similarities to other existing responsibilities and individual aptitudes and try to accommodate them.

Remember too that technical jobs are not just technical: an element of administration is essential.

Updating records, procedures, diagrams, fault logs, solutions and knowledge bases, in addition to providing reports, are vital aspects of all roles and should not be neglected.

In FITS there are likely to be more roles than there are people. This means that some roles must be combined for one person to carry out. As a rule, you will find that the roles in FITS can be defined as three types – managerial, technical and administrative.

## Technical support strategy

There should be a technical support strategy outlining how the service will meet the overall ICT strategy requirements. It may include:

- roles and responsibilities in the team
- supplier selection
- developing mechanisms for handling incidents
- new requirements
- new software testing and implementation
- hardware upgrading
- overall tracking of licences, equipment etc.

To define your technical support strategy you should answer these questions:

- What are the ICT services provided?
- What technology is required?
- What resources are required?

Resources are the people, time and money involved in supporting the technology and the services. It is important to understand the resource requirement. This will assist with deciding on staffing levels and what is supported in house or by external suppliers.

## Measuring the performance of technical support

It is important to measure both the actual service delivered to users (external metrics) and the effectiveness of processes used by technical support in this delivery (internal metrics). This will highlight current performance and identify potential issues and improvements that could be made.

Use measurements, but remember that the ICT user will judge performance on perception, not hard facts. You may be able to prove that a service was available 95% of the time, but if an ICT user rings the service desk and the telephone wasn't answered, their perception of the service will be poor.

## Tools for technical support

Tools are the software, techniques, equipment and information that help you provide good technical support. You can buy some that are ready to use immediately or configurable to your requirements. Certain ones are manual techniques you can follow; others are for you to create yourself. Here are several key tools you may like to consider.

### Process tools to help support the processes

- Software to manage the logging and resolution of incidents
- Software to manage the change management workflow
- Software to record configuration and asset details
- Software to generate workload and performance monitoring reports

### Knowledge bases for accessing useful information

- Technical knowledge base
- User handbook and technical support charter

### Specialist tools – for performing specific technical functions

- Network monitoring software
- Disk-imaging software
- Auditing software



## Service Desk

The service desk acts as a single point of contact between ICT and users, where they can submit enquiries, log incidents, obtain help and request change. The service desk not only handles incidents, problems and questions, but also provides an interface to users. Dealing with requests for equipment moves, software installations and help on how to use a system are typical service desk functions. The single point of contact at the service desk can perform some aspects of financial management and configuration management while also helping with the production of reports and administrative functions in other areas of FITS.

### Why a service desk?

Computer systems can grow very large from small beginnings. This often appears to happen overnight without being planned and takes users and technicians by surprise. Eventually the management and support of such an environment becomes very expensive, time consuming and frequently an exercise in futility.

There is nothing more frustrating than calling for technical support and getting passed around until you find the right person to speak to – provided, of course, they are not at lunch, on holiday or have just gone home.

### Benefits of a service desk in a school

- A common way of logging incidents and requests means that users know who to contact when they need help, incidents only require reporting once and the right information is always collected.
- Using a common shared call log helps with incident resolution, tracking logged calls to resolution and monitoring service levels.
- Familiarity with hardware, software and infrastructure aids quick resolution of incidents, and ensures that users receive appropriate training and that software and hardware standardisation can be maintained.

### Roles and responsibilities

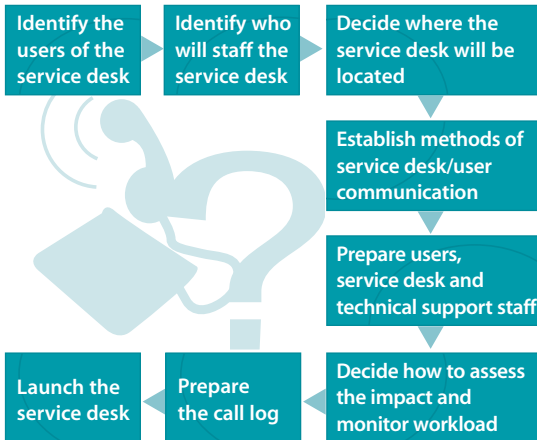
Any school that needs to understand its technical support requirements will start with implementing a service desk. This will help to put all technical requirements through a single point of contact, enabling needs, and how they are currently being addressed, to be understood.

### Who should staff the service desk

- A person with good interpersonal skills
- A person who is not providing technical support
- A person who is not necessarily technical but does need to be organised
- A person who could be performing another role (in a small school)

Remember the goal of the service desk is to enable the person providing technical support to concentrate on that work and not the details of how to log a call.

## How to implement a service desk



## How to operate the service desk

### Non-technical

If a non-technical person is staffing the service desk, they can solely log, track and update technical support calls. However, there is an opportunity to develop the role to encompass non-technical aspects of roles in other FITS processes including:

- configuration management database administrator
- financial administrator
- service continuity recovery team member.

### Technical

If a person with technical understanding is staffing the service desk, they may be able to carry out incident management. In many cases, this would speed up incident resolution and reduce technician workload.

## What you should achieve through the service desk

- A standard way of recording and logging incidents and requests
- A method of communication between the user and technician via the service desk
- Historical information about calls and failure rates of individual equipment
- Reports and feedback on the calls logged and resolved
- Knowledge about the time taken to resolve incidents and requests
- Information about calls currently outstanding and how long they have been logged



## Incident Management

Incident management is a defined process for logging, recording and resolving incidents. The goal is to restore the service as quickly as possible. This is often through a workaround or temporary fix, rather than trying to find a permanent solution. Detecting the underlying cause and permanent solution is the responsibility of problem management. Incident management should ensure that all details are recorded, so if a permanent solution is needed, problem management is able to continue once a workaround has been implemented.

### Why use incident management?

Wherever ICT is used, technical support will always have a reactive workload dealing with reported incidents. This could include fixing faults, helping users and acting on requests. When a computer stops working, the user is unable to continue their work, which could affect either teaching and learning or administration tasks within the school. Restoration of the ICT service as quickly as possible is therefore vital to minimise the impact and allow the user to work as normal.

### Benefits of incident management

- It reduces the impact of incidents on the school.
- Incidents are dealt with quickly, before they become severe.

- Incidents can be diagnosed quickly using previous knowledge, rather than treating each event as a new one.
- Knowledge of the configuration and changes made enables the cause of incidents to be identified quickly.
- Technicians can prioritise their workloads.
- Logged incidents will be addressed and not forgotten.

### Roles and responsibilities

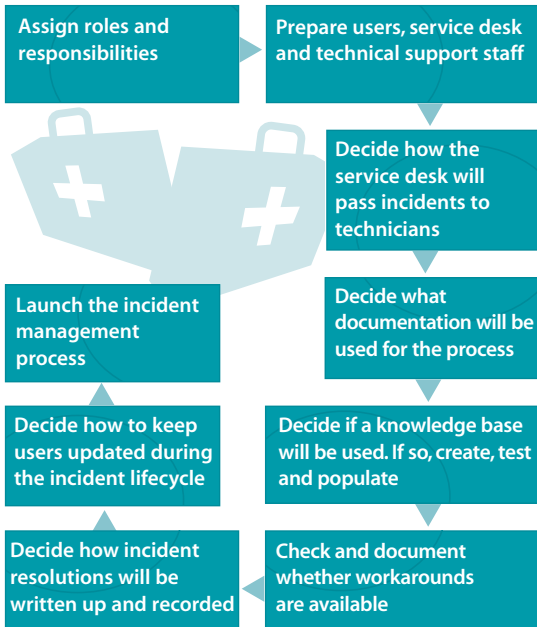
The staff mainly involved in carrying out incident management would be:

- competent users within the school who discover, try to repeat the conditions and report the incident to the service desk with the relevant details
- the person staffing the service desk (the single point of contact) who records the details in the call log, performs initial diagnostics, requests technician assistance and monitors the call through to closure
- technicians and other technical support staff who perform diagnostics, update the incident sheet and resolve the incident.

The service desk should be in place before implementing an incident management process.

If the incident is resolved with a temporary fix or workaround and a permanent fix is deemed necessary, the incident becomes a problem and is passed to the person responsible for problem management.

## How to implement incident management



## How to operate incident management

- A user discovers the incident, repeats the conditions and reports the incident to the service desk with the relevant details.
- The service desk logs the incident and may carry out the initial investigation by using information previously logged or the knowledge base.

- If this does not resolve the incident, the service desk will pass it to the technician and provide the necessary details.
- The technician will carry out diagnostics by using tools or identifying a known error, and will restore the service as quickly as possible.
- If a workaround was used to restore the service, the incident becomes a problem and is passed to the person responsible for problem management.
- The incident is closed and the resolution details entered in the call log.

## What you should achieve through incident management

- A consistent approach to handling incidents and how the response to the incident is planned
- Information about the number of calls currently outstanding and how long they have been logged
- Quick diagnosis and resolution of incidents by using information in the call log or knowledge base and from known errors
- Quick restoration of ICT service to users through workarounds
- Established process to escalate underlying network problems so permanent fixes are not overlooked



## Problem Management

The goal of problem management is to minimise both the number and severity of ICT incidents and problems in your school. Finding permanent solutions to underlying infrastructure problems will reduce the impact of incidents and problems, prevent their recurrence and help with future resolutions. A problem can be the occurrence of the same incident many times, an incident that has an impact on many users, or the result of network diagnostics revealing systems not operating in the expected way.

### Why use problem management?

Owing to the complexity of ICT infrastructure, underlying problems will always occur which can affect reliability and availability of the ICT service. Often it is possible to resolve an incident by using a temporary fix or workaround, but if the underlying cause is not resolved, the incident may recur or become more severe. Problem management uses a standard approach to find the underlying cause of the problem and record the resolution to help resolve future incidents.

### Benefits of problem management

- A standard way to approach every problem
- A reduction in the number of incidents

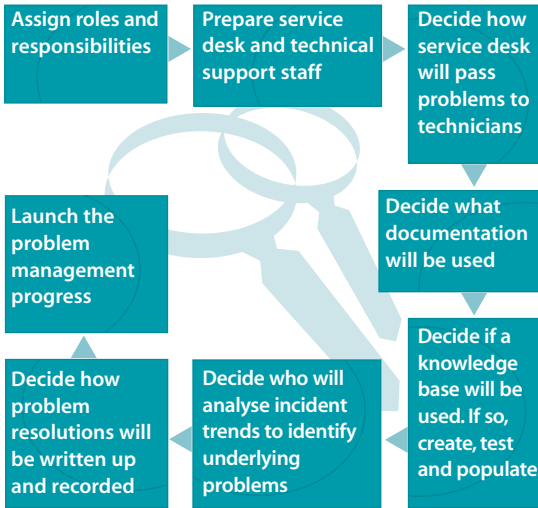
- Permanent solutions – there will be a gradual reduction in the number of problems and known errors, as those that are resolved stay resolved
- Learning from experience – the process provides historical data to identify trends, the means of preventing failures and of reducing the impact of failures
- Better first-time fix rate of incidents with a knowledge database available to the service desk and technicians when a call is first logged

### Roles and responsibilities

The staff mainly involved in carrying out problem management would be:

- the person staffing the service desk (the single point of contact) who passes the problem to the person responsible for problem management; logs, monitors and tracks the progress of the problem; and analyses incident trends to spot underlying problems
- technicians and other technical support staff who progress unresolved incidents, via the service desk, through to the problem management process and action the problems; assist with handling major incidents and identifying the root causes; prevent the replication of problems across systems; and escalate to second- and third-line support groups, including specialist support groups and external suppliers.

## How to implement problem management



## How to operate problem management

The service desk or a technician will perform diagnostics on an incident and decide whether it is really a problem. It is a problem if:

- the same type of incident has been reported on several other computers in the last few days
- the same type of incident has been reported on this computer in the last few weeks
- another fault has been reported on the same computer on a regular basis.

The service desk will contact the problem management technician and provide relevant details. These are the steps to take.

- The technician carries out problem analysis to find root cause.
- The technician produces a theory for what is happening or what has happened.
- The technician records all steps taken to resolve the problem which will help in future situations.
- If the resolution requires a change to the ICT infrastructure, you use the change management process.
- The problem is closed and resolution details entered in the call log.

## What you should achieve through problem management

- A formal process for dealing with problems
- A systematic method for deciding when an incident becomes a problem
- Information about the amount of technician time required to resolve problems
- A consistent approach to recording the actions taken as part of problem management and the results of the resolutions applied
- Information at your fingertips about the number of problems currently outstanding and how long they have been logged
- A process for checking whether problem management reduces the 'top 10' list of commonly reported incidents



## Change Management

Change management is the process for managing the implementation of changes to the ICT infrastructure including hardware, software, services or related documentation. Its purpose is to minimise the disruption to ICT services caused by change and to ensure that records of hardware, software, services and documentation are kept up to date. A change may be the result of a technical failure or problem dealt with in problem management. Alternatively, it could be because of a new ICT software or hardware requirement. In this instance the release management process would be the mechanism for defining and developing the new service and ensuring its readiness for implementation.

### Why use change management?

In every ICT infrastructure there will always be a need to make changes. Some of these could be:

- replacing a faulty switch
- installing a new software application
- installing additional memory in a server
- revising a procedure document.

Any change means introducing a risk of the change failing or causing something else to fail. Change management is proactive technical support focused on preventing incidents and problems by effective planning.

### Benefits of change management

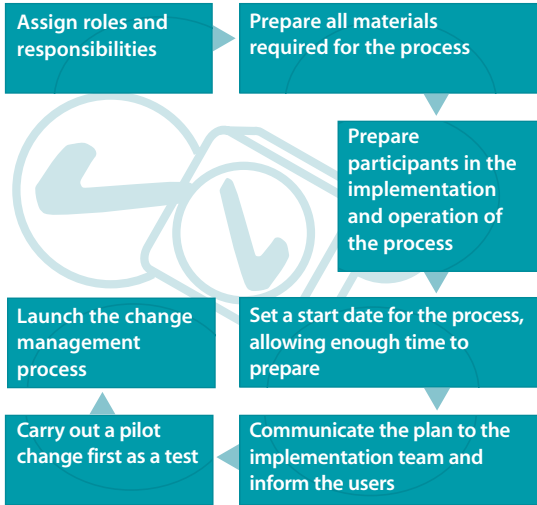
- Consistent planning for change
- Communication with appropriate parties before change occurs
- Approval received from appropriate parties before change occurs
- Reduction in incidents and problems caused by unplanned change
- Time spent on preparation and prevention rather than fire fighting and downtime

### Roles and responsibilities

There are a number of roles to be assigned in change management and those likely to fulfil them are the:

- originator – responsible for requesting technical changes – may be a technician, ICT co-ordinator, network manager or supplier
- initial approver – assesses the cost and value of proceeding with the change – may be the ICT manager, ICT co-ordinator or network manager
- peer reviewer – assesses the change and implementation plan for technical suitability and robustness – may be another technician, network manager or supplier
- final approver – seeks the views of affected or relevant user representatives to take part in this decision-making process – may be the headteacher, ICT manager or ICT co-ordinator
- implementer – implements the change in accordance with the plan and the scheduled date and time – may be a technician, ICT co-ordinator, network manager or supplier.

## How to implement change management



## How to operate change management

- Identify the change.
- Create a new request for change.
- Get approval to proceed from the initial approver.
- Plan and prepare the change.
- The peer reviewer assesses the change.
- The final approver gives approval to implement the change.
- Communicate the change with relevant details to the affected users.
- Implement the change and record whether it was successful.

- Update the records in the configuration management database.
- Close the change and retain the paperwork for future reference.
- Monitor the number of requests for change received.

## What you should achieve through change management

- There is a way of recording and keeping track of changes made.
- All major changes (to shared infrastructure items such as servers, routers, network cabling, other communications links and so on) are planned, approved and scheduled in accordance with the request for change process.
- You have an established method for handling requests for change – either by circulating the request for change to participants in the process or by holding regular meetings of a change advisory committee.
- Changes are implemented in a timely manner.
- Information about the number of changes being made is available.
- Changes can be considered within a bigger scheme context (the whole-school strategy/business plan) and you take the most appropriate action for the long term.



## Release Management

Release management is the process of planning, building, testing and deploying hardware and software, and version control and storage of software in a DSL (definitive software library). The DSL is a repository for storing released software and serves as the central point for obtaining software versions for installation. The goal of release management is to ensure that a consistent method of deployment is followed. It reduces the likelihood of incidents resulting from rollouts and ensures that only tested and accepted versions of hardware and software are installed.

### Why use release management?

Since ICT has been used in education, schools have looked for ways of using new technology to enhance teaching and learning. Computers have become more powerful, software applications more functional and new hardware such as whiteboards, tablets and PDAs are now available.

Introducing new hardware and software comes with its own risks. Will it be compatible with your current infrastructure? Will it offer the functionality you are expecting? Will the users require training before it is installed? These questions should be answered before anything new is released for use in the live teaching and learning environment to minimise the risk.

### Benefits of release management

- A structured approach to rolling out all new software or hardware
- Testing before rollout to minimise incidents affecting users
- An opportunity for users to accept functionality of software before it is fully implemented
- Advance training, so users do not experience system downtime while learning new features
- Version control and central storage of software, ensuring that correct versions are installed, minimising incidents and the need for reinstallation

### Roles and responsibilities

There are four roles in release management and those likely to fulfil them are:

- release manager – responsible for ensuring that the process is followed – may be the ICT manager, ICT co-ordinator or network manager
- build developer – responsible for integrating new hardware or software into existing services – may be a technician, ICT co-ordinator, network manager or supplier
- acceptance tester – responsible for confirming that the new hardware or software performs the functions it was obtained for – may be a teacher, teaching assistant, staff member or any end-user
- installer – responsible for performing day-to-day installations of hardware or software – may be a technician, ICT co-ordinator, network manager or supplier.

## How to implement release management



## How to operate release management

- Request installation of build. This will happen via the incident/request process in incident management or the request for change process in change management.
- Create build using the procedure template, which includes design, build, test and accept.

- Release build using the procedure template, which includes storing software in DSL, storing documents and recording in configuration management database, and communicate availability.
- Install build using the checklist, which includes install details, install checklist and install document details.

## What you should achieve through release management

- Fewer ad hoc requests for new hardware or software
- All hardware and software installations tested and documented
- Hardware and software installed consistently each time
- Less time spent resolving incidents and problems caused by badly installed hardware and software
- All software stored centrally
- Correct and current software versions clearly identifiable
- A list of all software licences
- Details of to whom or what each software licence is assigned



## Configuration Management

Configuration management is the process of creating and maintaining an up-to-date record of all the components of the ICT infrastructure. The 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. The extra value is the rich source of support information it provides consistently to all interested parties. This information is stored together in the configuration management database (CMDB).

### Why use configuration management?

There are many components in an ICT infrastructure – for example servers, switches, routers, computers, laptops and printers. One of the main difficulties of ICT management is identifying what equipment you have, where it is and how it connects together, especially as equipment is moved around or replaced as part of normal operation.

Accurate records of the ICT infrastructure are useful for insurance and asset valuation, but their main purpose is to help you understand the infrastructure and make informed decisions, and also to assist in the speedy resolution of incidents.

### Benefits of configuration management

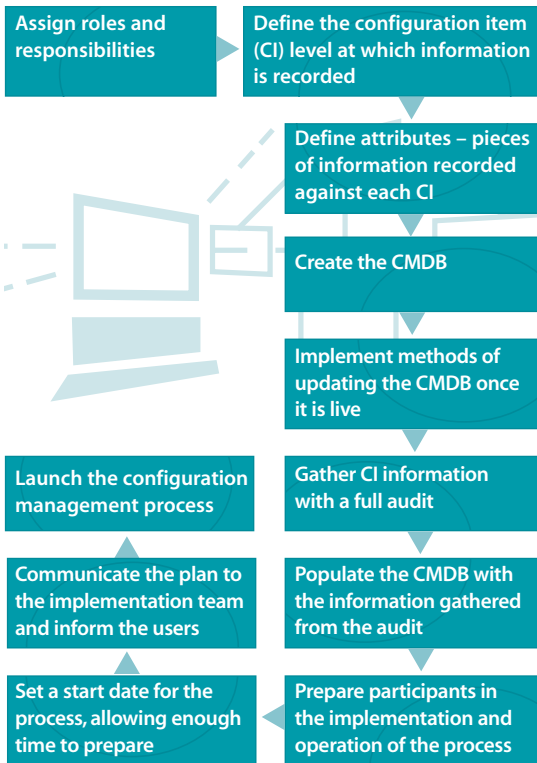
- Technical information is available to ICT staff and suppliers.
- Dependencies between configuration items are understood.
- The information available helps in the planning of changes.
- There is a single, consistent, source of information.
- Graphical representation of the infrastructure is available to aid diagnosis of incidents and problems.
- When supported by change management, the CMDB is kept up to date.
- It provides an asset list.

### Roles and responsibilities

There are three roles in configuration management and those likely to fulfil them are:

- configuration manager – with overall responsibility for configuration management or ICT in general – may be the ICT manager, ICT co-ordinator, network manager or technician
- CMDB administrator – responsible for maintaining the configuration management database – may be a technician, ICT co-ordinator or secretary/administrator
- implementer – responsible for carrying out technical changes – may be a technician, ICT co-ordinator, network manager or supplier.

## How to implement configuration management



## How to operate configuration management

- Update the CMDB – it must be continually updated (with all additions, moves, removals and changes to configuration items). Failure to do so will result in meaningless information.
- Audit and verify the configuration items. Carry out periodic checks to ensure that the CMDB contents reflect the reality of the infrastructure.
- 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 published in a report.

## What you should achieve through configuration management

- You keep a record of all ICT assets.
- The processes for keeping this record up to date are all 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.
- The age of equipment and planning for its replacement is identified.
- Equipment that has been assigned to departments and individuals is accounted for.
- Technical support has a basis for understanding the relationships between ICT components.
- An effective CMDB update process means few amendments are needed after an ICT audit.



## Availability and Capacity Management

Availability and capacity management in ITIL are two separate processes:

availability management and capacity management. Both processes focus on the proactive detection and prevention of ICT problems. They help you to optimise what you have and to decide what you need. We have streamlined these themes into two processes that span both availability and capacity management. They are network monitoring and preventative maintenance, terms that should sound more familiar to you.

### Why use availability and capacity management?

Availability and capacity management allows your ICT end-users to depend on the ICT services they have become accustomed to. If they rely on ICT to carry out activities, the ICT infrastructure must be reliable enough for this to happen whenever it is needed, not just some of the time.

### Benefits of availability and capacity management

- ICT infrastructure is maintained to prevent the occurrence of failure as far as possible.
- Potential problems are seen before they become problems.
- The design of the ICT infrastructure is improved and single points of failure eliminated.
- It detects failures quickly.
- It diagnoses failures.
- Peaks and troughs of infrastructure utilisation are understood and optimised accordingly.



## Preventative Maintenance

In order for your network to work properly, every component of the network must work properly. Preventative maintenance is concerned with anything that can be done to prevent any component of your network from failing.

### Why use preventative maintenance?

Research shows that the cost of maintaining and operating ICT equipment over the lifetime of the components can be at least double the initial outlay. An effective preventative maintenance programme can drastically reduce the cost associated with the day-to-day operation of the equipment.

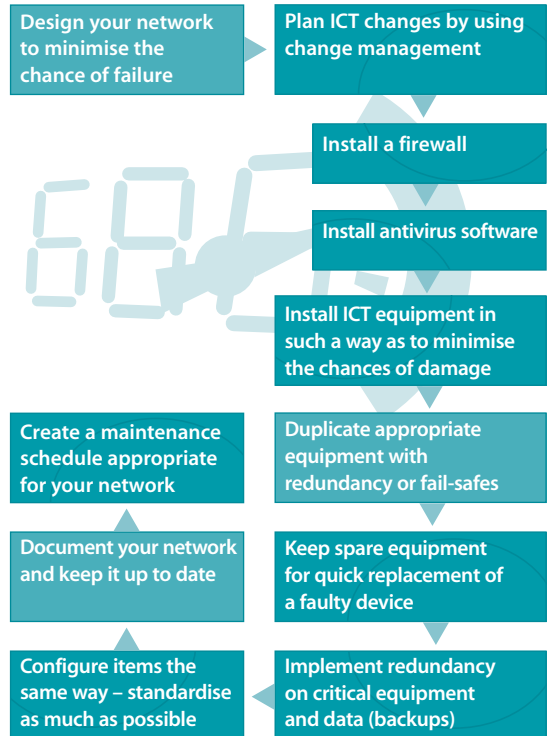
Implementing a preventative maintenance programme enables you to detect and prevent many problems before they become user-reported incidents, by ensuring that the individual components that comprise your network are operating as reliably as possible.

### Benefits of preventative maintenance

- Increased availability of ICT as a result of reduced network downtime
- Increased life expectancy of network components, eliminating premature replacement of parts
- More economical use of technical staff as they are working to a schedule, rather than reacting to repair breakdowns
- Lower repair costs, because there will be fewer secondary failures (when parts fail in service they often damage other parts)

- Reduced product rejects, rework and scrap, owing to better overall equipment condition
- Identification of equipment with excessive maintenance costs, indicating the need for corrective maintenance, operator training or replacement of obsolete items

### How to implement preventative maintenance



## How to operate preventative maintenance

- Ensure that the maintenance schedule is adhered to.
- Report any errors discovered during routine maintenance as incidents to ensure that their detection, diagnosis and resolution are recorded.
- Ensure that any changes made to the network are reflected in the maintenance schedule.
- Keep antivirus software, backups and security up to date.

## What you should achieve through preventative maintenance

- Fewer major outages on your network due to redundancy in critical equipment such as servers, network paths and internet connections
- Quicker resolution of incidents by using equipment spares
- Better protection for your network with firewalls and antivirus software
- Fewer failures caused by environmental and physical damage
- Improved life expectancy and reliability of network components reducing replacement costs

## Network Monitoring

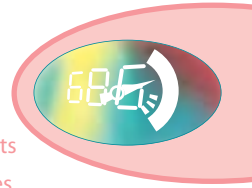
Network monitoring deals with the detection of infrastructure activity and its impact on the components. This includes identifying capacity issues, establishing trends in usage peaks and troughs and finding points of failure that may have already occurred – ideally before an end-user reports it to the service desk.

### Why use network monitoring?

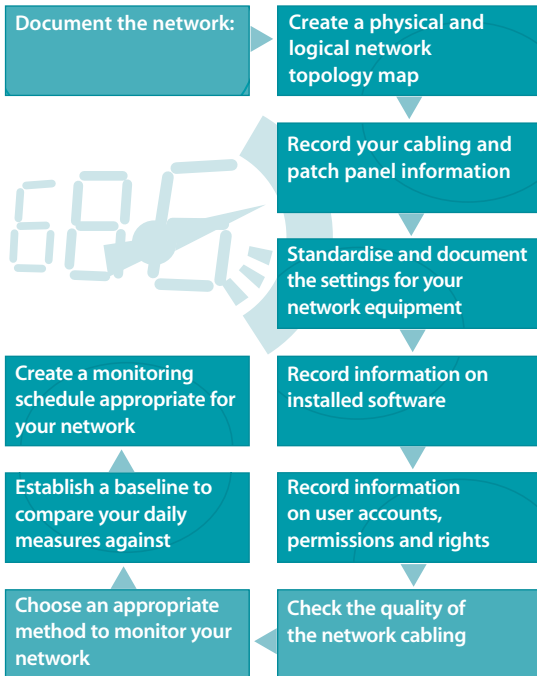
Such a system can monitor the entire school network for critical events that may interrupt service and cause loss of time and resources. The collection of data on historical and current usage, remaining capacity and system failures enables you to identify and analyse trends. This information provides a valuable input to the ICT strategy and budgeting process. While you can do some network monitoring manually, suitable network monitoring software is more efficient and thorough, and will produce reports, graphs and measurements for the leadership team.

### Benefits of network monitoring

- It helps to ensure the network is available to users.
- You can respond more quickly to incidents and problems.
- It helps to determine where the network is performing well or otherwise.
- It identifies trends and determines how to optimise the network by changing network configurations or replacing network devices.
- It improves the visibility of network status.



## How to implement network monitoring

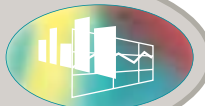


## How to operate network monitoring

- Check server error and usage logs to identify potential problems.
- Check and record server disk space to identify potential problems and trends. This can highlight the need to free up additional space or install a new hard disk.
- Produce and collate management reports on network usage and performance.
- Identify trends and determine how to optimise the network by changing configurations or replacing network devices where necessary.
- Report any errors discovered during routine maintenance as incidents to ensure that their detection, diagnosis and resolution are recorded.

## What you should achieve through network monitoring

- Improved efficiency in resolving incidents and problems due to accurate labelling of cabling and network equipment
- Proactive detection and resolution of underlying issues relating to cabling, network traffic, failing network equipment and server capacity
- Requirements for additional disk, network traffic or processor capacity identified and planned



## Service Level Management

Service level management is the process of ensuring that ICT services are supported to an acceptable level. It involves understanding the ICT requirements of the end-users and working within the constraints of available resources. The result is an agreed, consistent level of service that end-users can come to expect. This agreement is between those responsible for ICT and the end-users, who are usually represented by one or more people from each area or department. Once agreement is reached, the service level management process facilitates the creation of underpinning agreements with third parties involved in the service provision.

### Why use service level management?

ICT provides a number of services to users such as internet access, email, printing and data storage. Different end-users may have different requirements from each service. Availability and how quickly someone will respond to a reported fault are typical examples. So from a support viewpoint, it is important to know what services you provide, when they are required and whether you have the resources to provide them at the level required. By agreeing the level of service in advance, you set expectations and avoid possible conflict between the users and the technical support providers.

### Benefits of service level management

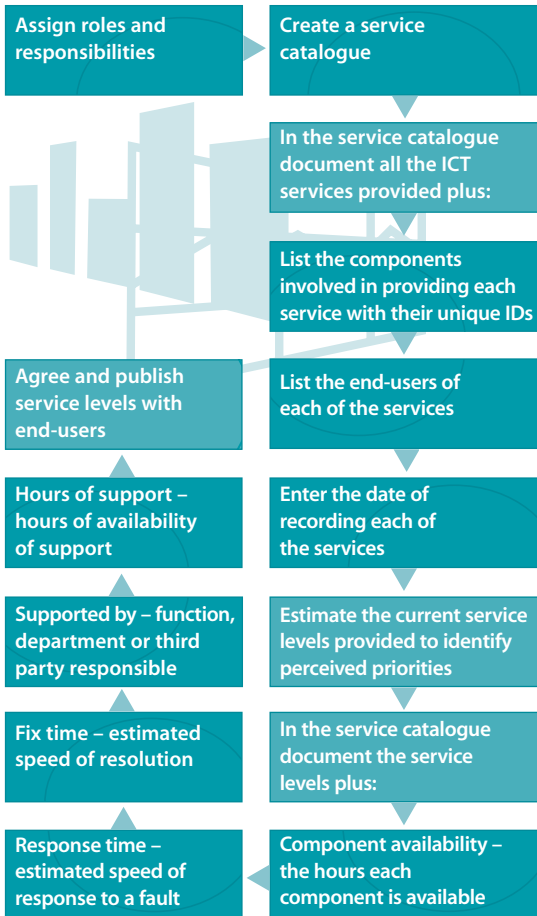
- It highlights what services are already in place.
- It helps to determine priority services.
- It indicates a clear remit for those providing technical support.
- It helps to allocate resources appropriately.
- It determines a minimum acceptable level of service.
- It helps to highlight shortcomings in service provision.
- It provides a basis for discussion and promotes communication.
- It provides targets to aim for.

### Roles and responsibilities

There are two roles in service level management and those likely to fulfil them are:

- service manager – with overall responsibility for the technical support or ICT provision – may be the ICT manager, ICT co-ordinator, network manager or technician
- end-user representative – responsible for representing the end-user ICT requirements – may be the headteacher, teacher, teaching assistant, student or administrator.

## How to implement service level management



## How to operate service level management

### Capture some real data

To build on the 'guesstimate' measurements added to the service catalogue when working through the service level management implementation, you need to capture some real data from each of the FITS processes. For example, for each month:

- number of incidents logged
- average time to incident resolution
- number of incidents resolved by service desk
- number of requests for change processed.

### Produce a service report

The report should include the period covered plus reactive, proactive and change statistics.

### Review service levels

Use the information in the service report to identify potential issues and areas requiring further investigation. Monitor trends over a period of time and look for fluctuations.

### What you should achieve through service level management

- A catalogue of authorised ICT services, which are always kept up to date
- A clearer picture of service levels being provided
- Target service levels to aim for
- Regular creation and review of service reports
- Regular review meetings with end-user representatives
- Findings from reports and review meetings that result in an improved level of service



## 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 should seriously affect or destroy the 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 – not just the continuation of equipment.

### Why use service continuity management?

In an uncertain world, it is difficult to know what is around the corner. Often we hear of major fires or the risk of flooding which could have an impact on the normal operation of a school, including the ICT service. The risks are not confined to these dramatic and remote-sounding examples. There are many more commonplace possibilities:

- severed cable under road
- leaking central-heating system
- destructive software virus
- transport difficulties affecting staff
- loss of a system password.

Schools can take steps to reduce the risk of these events on the ICT service by preparing efficient recovery plans in readiness.

### Benefits of service continuity management

- 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 of a medium- to long-term ICT outage on school activities.
- Good service continuity management can help reduce insurance costs.
- It allows technical support to understand the importance and priority of ICT services within the school, which is beneficial day to day, not just in the event of a disaster.

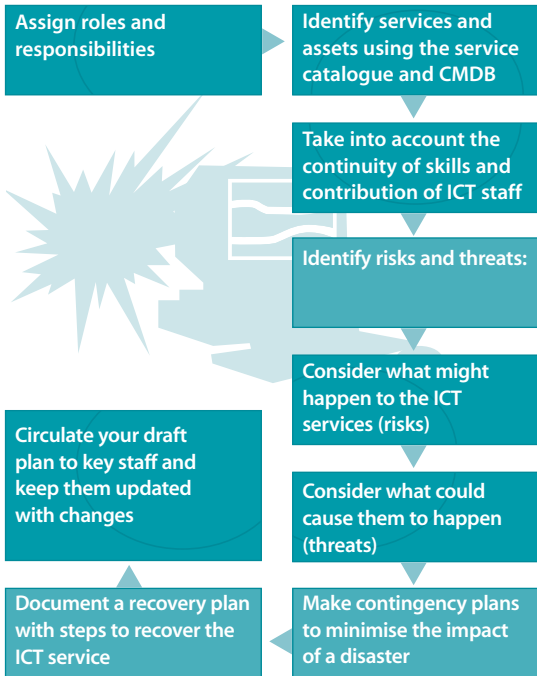
Don't think 'it won't happen to me'. Service continuity management is not just for dramatic disasters – workaday accidents do happen!

### Roles and responsibilities

There are two roles in service continuity management and those likely to fulfil them are:

- service continuity manager – with overall responsibility for the technical support or ICT provision – may be the ICT manager, ICT co-ordinator or network manager
- service continuity recovery team – people involved in the service-continuity recovery plan – may be a technician, teacher, ICT co-ordinator, administrator or ICT users.

## How to implement service continuity management



## How to operate service continuity management

You must review your service-continuity recovery plan on a regular basis and carry out the following.

**Keep the plan up to date** in line with changes to services and assets. This is managed via other FITS processes:

- configuration management – the CMDB should always hold the latest asset information
- service level management – service catalogues and service-level agreements should have up-to-date details of services in use and service levels required
- change management – the process that ensures that other data sources are 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.

**Improve the plan** – keep reviewing what you have done so far and consider what improvements you can make.

**Improve countermeasures** – review your risks and threats and take action to reduce the possibility that they will occur.

## What you should achieve through service continuity management

- A service catalogue documenting all ICT services
- A contingency plan that can be invoked in the event of a disaster or accident
- The contingency plan rehearsed with all participants
- Copies of your contingency plan kept securely on and off site
- The contingency plan kept up to date with changes to ICT services and user requirements
- The risks and threats to ICT services neutralised



## Financial Management

FITS financial management is the tracking and control of ICT services and support costs. In its entirety, it also covers cost recovery as a means to place accountability for ICT costs on the users of the service. The purpose is to ensure that the costs are justifiable. This process also helps to identify particularly costly areas that you may want to examine to see if a different approach might reduce costs.

### Why use financial management?

There is always a cost involved in providing an ICT service in a school. The costs can be made up of hardware, software and the resources required for management and support. Without sound financial management, it is possible for these costs to become excessive and unsustainable. Financial management helps you to record the cost of providing ICT and ICT technical support.

### Benefits of financial management

- You can account for all money spent on ICT equipment.
- Knowing how much money is left in the budget helps you to decide whether you can meet any unplanned expense.
- You can identify expenditure on items not budgeted for, to prevent overall overspend.
- Budgeting becomes increasingly accurate as financial information improves.
- Being able to see patterns in spending can highlight potential cost savings such as bulk buying.
- Keeping a record of expenditure helps to highlight any problem areas such as unauthorised purchasing.
- You can see the bigger picture of how money is distributed across ICT requirements.

### Roles and responsibilities

The two roles in financial management and those likely to fulfil them are:

- financial manager – with overall responsibility for the technical support or ICT provision – may be the ICT manager, ICT co-ordinator or network manager
- financial administrator – the person authorised to spend money, as determined by policy in the individual school – may be a technician, teacher, ICT manager or ICT co-ordinator.

## How to implement financial management



## How to operate financial management

On a day-to-day basis, you need to maintain the expenditure record, monitor your expenditure and make decisions for improvements to financial management.

## Maintaining your expenditure record

For it to be of value, the expenditure record must be kept up to date.

## Monitoring expenditure

It is important that you use the expenditure record information to monitor where and how money is being spent.

## Making decisions

Use the expenditure records to identify areas where it may be possible to make cost reductions.

## Budgeting ahead

While you may not be able to dictate the size of your ICT budget, you can at least plan how to spend the amount you receive. This is where your previous expenditure records will be useful.

## What you should achieve through financial management

- Details of all financial transactions relating to ICT equipment and services are recorded.
- You have a clear picture of how much money has been spent on ICT at all times.
- ICT budgets include expenditure required on supporting items, not just hardware and software.
- ICT budgets are refined each budgetary period, using the records of actual expenditure from the previous or current period.
- Regular expenditure reports are produced.

## Further guidance and contact points

The FITS Pocket Guide is the latest in our series of ICT Technical Support products. Other products under development are FITS Training and FITS Online Assessment. Current information and products are freely available on the Becta website. If you wish to keep abreast of our latest developments, you can register to receive updates.

<http://www.becta.org.uk/leaders/technicalsupport>

You will also find the following documents available for download:

FITS Introduction  
(last updated April 2004) (PDF 413 KB)

Service Desk  
(last updated April 2004) (PDF 227 KB)

Incident Management  
(last updated April 2004) (PDF 331 KB)

Problem Management  
(last updated April 2004) (PDF 246 KB)

Change Management  
(last updated April 2004) (PDF 332 KB)

Configuration Management  
(last updated April 2004) (PDF 276 KB)

Release Management  
(last updated April 2004) (PDF 317 KB)

Availability and Capacity Management  
(last updated April 2004) (PDF 55 KB)

– Network Monitoring  
(last updated April 2004) (PDF 434 KB)

– Preventative Maintenance  
(last updated April 2004) (PDF 325 KB)

Service Level Management  
(last updated April 2004) (PDF 252 KB)

Service Continuity Management  
(last updated April 2004) (PDF 229 KB)

Financial Management  
(last updated April 2004) (PDF 259 KB)

Through FITS, Becta aims to improve the reliability and stability of the ICT infrastructure in schools to ensure maximum availability for teaching, learning and administration. Our online community for schools' ICT support professionals is available at [<http://www.becta.org.uk/technicalsupportcommunity>].

Becta is the Government's lead agency for ICT in education. Working to support the development of ICT in education throughout the UK, Becta's unique contribution is to combine knowledge of the needs of education with an understanding of the power of technology.

© Becta 2004

You may reproduce this material free of charge in any format or medium without specific permission, provided you are not reproducing it for profit, or for material or financial gain. You must reproduce the material accurately and not use it in a misleading context. If you are republishing the material or issuing it to others, you must acknowledge its source, copyright status and date of publication.

Publication date: September 2004

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.