# FITS OM
# pocket guide

A handy reference guide to
ICT operations management in schools

**http://www.becta.org.uk/schools/technicalsupport**

Becta
ICT Advice

## About this guide

This pocket guide is designed as a handy reference book for everyone involved in ICT management or day-to-day technical support in schools. Anyone defining ICT or technical support strategy in schools will also find it helpful. The guide is complementary to the Framework for ICT Technical Support Operations Management (FITS OM), developed by Becta and freely available on the Becta website **[http://becta.org.uk/fitsom]**.

In this guide we explain the importance of having effective operations management, the FITS OM functions and how they integrate with the FITS processes. We recommend that schools implement all the FITS processes to a level of maturity before undertaking the implementation of FITS OM. This is because the management of the FITS OM activities require the FITS processes to be in place.

Based on FITS OM best practice, the advice given in these guidelines is neither definitive nor prescriptive. It is applicable to all schools, however, and will be of benefit irrespective of size or the technology you use. You should adapt the guidelines and use them to meet your individual school's resources and needs.

The key message we want to stress is that operations management underpins efficient ICT service delivery because if your network technology is poorly configured and administered, it is likely to compromise the reliability of your ICT services.

# Contents

# Background to FITS and FITS OM

The national digital infrastructure is Becta's model for school networks **[http://becta.org.uk/schools/infrastructure]**. One of its aims is to ensure that each school has a reliable ICT infrastructure that will not only maximise the school's return on its investment, but also help the school to enhance the quality and effectiveness of its learning and teaching. Reliability is achieved through high-quality technical design, technical support and service provision.

Becta launched the Framework for ICT Technical Support (FITS) in September 2003 to help schools achieve high-quality technical support and service provision. A toolkit of advice, checklists and downloads, FITS **[http://becta.org.uk/fits]** offers technical support best-practice processes for managing the support and delivery of the ICT services that schools use in their learning, teaching and management.

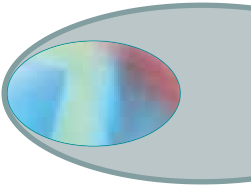
Schools that have implemented the FITS processes have benefited from:

- Increased reliability of the ICT services and delivery of technical support
- Improved user confidence in the ICT services and technical support provision
- A move from reactive to proactive technical support
- More efficient use of technical support resources
- Improved communications between technical support, users, senior managers and suppliers.

You can find more information on the impact and benefits of implementing FITS in the evaluation report published in January 2006 **[http://becta.org.uk/fits/evaluationreport]**.

The focus of FITS is the management and support of school ICT services. One of the less developed areas in FITS is the approach towards the operations management of the network technology in the ICT infrastructure. Operations management underpins sound ICT service delivery: it is only if you have well configured and efficiently administered network technology that you can ensure reliable ICT services. This is why we decided to develop FITS OM.

# Introduction to FITS OM



To help schools put in place effective operations management, Becta launched FITS OM, which is based on a collection of best-practice principles and models used successfully in education and industry. FITS OM is complementary to FITS and uses the same approach to help schools implement best-practice in bite-sized and manageable chunks.

We recommend that schools implement all the FITS processes to a level of maturity before tackling the FITS OM functions. This is because all the OM functions use the FITS processes to manage the activities within them.

For example, if technical support installs a new storage device following the function specification 'Storage Management', the FITS processes used would be as follows.

| | |
|---|---|
| **FITS Change Management** | **To document, assess, plan and approve the change** |
| **FITS Incident Management** | **To deal with faults, failures or breaches** |
| **FITS Service Level Management** | **To manage user expectations for data restores** |

To check whether your school has implemented all the FITS processes to a level of maturity, you may like to work through the FITS assessment **[http://becta.org.uk/fits/assessment]** or attend the Implementing FITS expert workshop **[http://becta.org.uk/fits/expertsworkshops]**.

FITS OM is Becta's structured approach designed to help schools to achieve operational excellence in managing and administering the technology of their ICT infrastructure. The technology comprises the network components that support the ICT services used for learning, teaching and management:

- Servers and computers
- Operating systems
- Routers, switches and firewalls
- Peripherals
- Cabling.

To be able to provide reliable ICT services for learning, teaching and management, you have to configure, operate and administer the network technology effectively. Poor practices will have a big impact on reliability and availability of ICT services, because:

- Network components and services may not work efficiently
- Security could be compromised, and this would affect availability
- Recovery from an ICT service interruption, such as a fault or disaster, could be difficult.

Tailored specifically for schools, FITS OM offers a quick-start approach to implementing best practice with any type of technology, platform or infrastructure.

## FITS OM functions

In FITS OM there are six functions, each covering a different area of best-practice operations management. A function – or specialist area of activity – has a complete and separate set of materials devoted to it.

| Systems Administration | | | | |
|---|---|---|---|---|
| Storage Management | Directory Services Administration | Print and Output Management | Security Administration | Patch Management |

Schools should carry out all the functions. If you do not, you risk compromising the availability, reliability and stability of your ICT services. Many schools will already be carrying out some or all of the functions in FITS OM. However, FITS OM brings together the operations management functions into one framework to help schools understand exactly what they or their suppliers should be doing.

As schools have limited resources, we expect that each technical support staff member will be allocated more than one of the FITS OM functions. For example, in a school with just a network manager to run the ICT services, he or she will have to carry out all of the functions. However, this is not a problem as long as that person has the necessary skills and dedicates the appropriate time to each function.

## Why have operations management functions?

The FITS OM functions both define all the activities to be carried out and also act as a benchmark to measure the effectiveness of existing operations management. In addition, the FITS OM functions help schools put in place the operations management policies they need. These policies determine how the technology is managed in order to support the ICT services. The activities in each function allow technical support staff to manage the day-to-day workload within the scope defined in the policies.

On the whole, the network technology and technical support in schools have tended to grow organically over time. Effective planning to cover all aspects of ICT infrastructure management has given way to constant reactive fire-fighting just to keep ICT services available as much as possible to the users in the school.

When they have time, most network managers and technicians have used their experience and knowledge to put in place activities to keep the network as available and reliable as possible. However, they do not always carry out some of the essential activities. This leaves the school vulnerable to network failures, poor performance and attacks by hackers that will have an adverse impact on the learning, teaching and management in the school.

## Approach to implementing FITS OM

Because their day-to-day activities are unpredictable and must take priority, ICT technical support staff often have little free time to spend on implementing processes, procedures and policies. In a school with an existing ICT infrastructure, however, you may find that many of the FITS OM functions are partly or fully in place and in use.

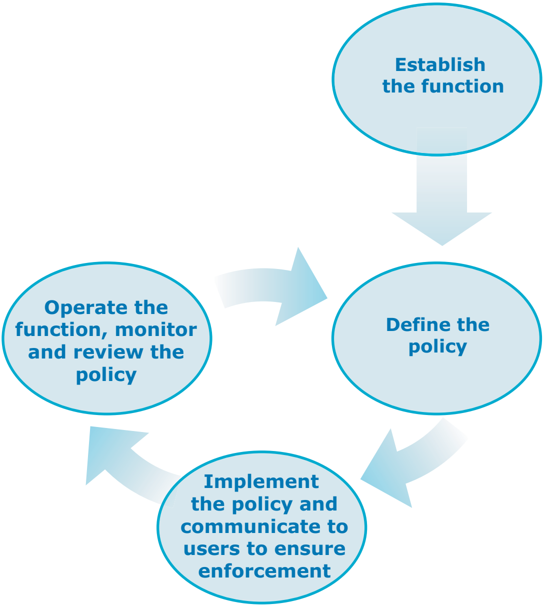
Our aim is to help you begin to remove some of the unpredictability you face, by introducing best-practice operations management functions in small steps. This will enable you to begin to realise the benefits of FITS OM as quickly as possible with the minimum impact on your normal activities.

FITS OM brings together all the best-practice functions and defines all the activities of the functions. This allows you to examine your school's existing practice and put in place the areas that are missing or rectify those that are not working effectively.

It is impossible to implement all the functions of FITS OM at the same time. In fact, Becta believes that a cyclic approach to implementation is beneficial, as it enables you to build solid foundations on which to develop your functions without spending an unrealistic amount of time on getting started. We at Becta have used our collective experience to apply the lessons we have learned over many years to develop this approach for schools to help you to implement best practice successfully from the outset.

## Cyclic implementation

This diagram shows the cycle of implementation for the FITS OM functions.


Establish the function
Define the policy
Implement the policy and communicate to users to ensure enforcement
Operate the function, monitor and review the policy

Your school may already have implemented a function in part or full, in which case this will affect your starting point on the cycle. If your school has not established a function, you should begin by gaining an understanding of that function and allocating roles to members of your technical support team or to external suppliers. Use the Systems Administration function to structure your school's technical support team and begin to allocate the activities.

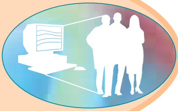
Once you have established the function and you are certain that the technical support staff understand their responsibilities, you can define and agree a policy with key stakeholders in the school. This may be a security policy, backup policy, directory services policy, printing policy and so on. The policy is intended to document how to set up and then configure the technology, and how to operate and use it to ensure that it remains available and secure.

Once defined and agreed, the policy needs to be implemented. Implementing the policy may mean not just changing the technology or its configuration, but also telling the users about it and making sure that they follow the policy and the associated new procedures. For example, your school may introduce a new backup-and-restore policy that requires users to request data restores in a certain way.

As soon as the policy is implemented, the function owner should start to carry out the day-to-day operations of the function, monitoring and reviewing the policy to ensure that it is working effectively, and constantly looking for improvements.

## Who is involved in FITS OM?

| Position | FITS OM role |
|---|---|
| School leader | • To put in place the required resources to carry out the FITS OM functions<br>• To provide support during the function's implementation and operation |
| Network manager | • To plan the implementation<br>• To define and draft the policy for each function<br>• To allocate the activities within each function<br>• To manage the implementation of the policy<br>• To monitor the activities and overall performance of the function<br>• To carry out the function activities allocated to them<br>• To review the function |
| Internal or external technical support staff | • To carry out the function activities allocated to them<br>• To report any function or activity issues to their network manager |
| ICT users | • To follow the agreed process for logging incidents or requests<br>• To adhere to the rules defined in the policies |



# Systems Administration

The goal of Systems Administration is to structure the internal and any external technical support resources in the most effective way to carry out all the activities of the FITS OM function. Systems Administration provides day-to-day administrative services in support of the technology in the ICT infrastructure.

The Systems Administration function manages the activities of Storage Management, Directory Services Administration, Print and Output Management, Security Administration, and Patch Management.

## Why use Systems Administration?

With the increase in size and complexity of networks and the demand for reliable ICT services in schools, it is now more important than ever to use technical support resources effectively.

Systems Administration helps schools to define the structure of their technical support team, allocate ownership and assign the activities of each function to staff with the appropriate skills. Without this structure, you may neglect some important areas and activities, which risks compromising your ICT services.

Most schools have limited technical support resources, whereas in industry, larger companies employ staff with specialist skills to manage each operations management function, such as security, backups or directory services. Schools therefore have to be more creative with their allocation of activities but, on the plus side, this gives technical support staff the opportunity to acquire skills and experience in all areas of operations management.

FITS OM has been specifically written for schools to enable you to implement best practice with limited technical support resources.

## Who is involved in Systems Administration?

| | |
|---|---|
| Network manager | • Defines the structure for the technical support team<br>• Allocates ownership of all FITS OM functions<br>• Allocates the activities in each of the functions |
| Senior technician | • Accepts and understands all activities allocated<br>• Reports function issues to the network manager |
| Technician | • Accepts and understands all activities allocated<br>• Reports function issues to the network manager |
| Service desk administrator | • Accepts and understands the administration activities allocated<br>• Carries out the single point of contact activities and communicates with users |
| Senior management | • Provides input and supports the network manager when defining the policies |
| Suppliers | • May carry out all activities of network manager and technicians if internal resources are not available |
| ICT users | • Adhere to defined policies<br>• Report incidents using the defined procedure |

## How Systems Administration works

To help you put in place the technical support structure to implement and operate the FITS OM functions, follow this flowchart.

Draw up a list of the available technical support staff

step 01

Include internal and external staff

Match their skill sets as closely as possible to the four defined levels A, B, C, D

step 02

A = Service desk administrator
B = Technician
C = Senior technician
D = Network manager

Appoint an owner for each of the FITS OM functions

step 03

In most schools the ownership for all functions will lie with the network manager. However, in a smaller school the ownership can be allocated to an external supplier.

Use the allocation table (provided within Systems Administration) to allocate the activities within each function to the staff, according to their level

step 04

On the list enter the allocated activities for each person and discuss it with them

step 05

Discussion is key to ensure that the person is comfortable with the activities and understands what they are.

When defining the policy for each of the FITS OM functions, include who is responsible for each of the activities

step 06

## Using Systems Administration to allocate the FITS OM functions and activities

Systems Administration has an allocation table to help schools allocate the activities in each of the FITS OM functions to staff in the technical support team **[http://becta.org.uk/fitsom/documents/sys_admin_allocation_table.doc]**. Using this will help you to structure your resources efficiently. It is based on a team of four with a skill set ranging from a non-technical service desk administrator through technician and senior technician to the network manager – with correspondingly increasing levels of technical knowledge.

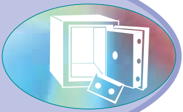
We realise that not all schools will have this many internal technical support staff, in which case you may have to combine some of the roles. For example in a school with two or three technical support staff you can consider the following options.

| Combining roles | But beware... |
|---|---|
| Service desk administrator and technician | This will increase the administrative burden on the technician, who will have less time for technical work. |
| Network manager and service desk administrator | This will increase the administrative burden on the network manager, who will not be able devote as much time to strategic and planning work. |
| Network manager and senior technician | A network manager with good technical knowledge should be able to do the senior technician work, but it will leave the manager less time for strategic and planning work. |

A school with only one full-time technical support staff or less is unlikely to have the capacity to carry out the activities in all of the FITS OM functions. In this case the school may want to ask an external supplier to take ownership of some or all of these. The following table gives some example approaches.

| Contracting out FITS OM activities to a supplier | Allocation of functions and activities |
|---|---|
| In a school with a highly technical network manager only | The network manager could retain ownership of all the FITS OM functions, but ask a supplier to provide assistance with some of the activities.<br>For example the network manager could define the policies and monitor them, but allocate the activities to an on-site technician provided by a supplier for a number of hours per week. |
| In a school with a less technically skilled network manager or technician only | The school could ask a supplier to take ownership of all of the FITS OM functions, define the policies for each and carry out the more technical activities.<br>The network manager could carry out the less technical activities such as incident management and maintenance tasks. |

| | |
|---|---|
| In a school with no technical support staff | The school would contract out to a supplier the ownership of all FITS OM functions and most of the activities.<br>It would be best for someone at the school to have enough understanding of FITS OM to know that the supplier is carrying out the right activities to the agreed levels of service. Also, it would be beneficial for the supplier to have an understanding of FITS OM so that both supplier and school talk the same language.<br>The school should carry out the service desk administrator activities, as it is important to keep a single point of contact in the school to manage the incidents and problems. |



# Storage Management

The goal of Storage Management is to define, track, and maintain data and data resources in the school's ICT environment. Storage Management is concerned with the operation and maintenance aspects of storage media and the data held on such media.

Storage Management is more than just performing data backups and restoration processes in the case of a data-related incident. It takes into account other activities such as archiving, selecting and maintaining storage media and tracking the school's important data.

## Why have Storage Management?

In a school, the main objective of information systems is to process data into information that helps the school to achieve its goals (via curriculum applications, presentations, administrative systems, email and so on). This data is kept in a data storage facility in the form of databases or files.

The real value of any ICT network lies in the data it holds, as it is this data that supports teaching and administrative activities for your school. Data is becoming an increasingly important asset of any school, so, like any other valuable asset, you need to protect it. Storage Management can mitigate risks to a school should the data become lost or unavailable.

## Roles and responsibilities

There are two roles in Storage Management: storage administrator and media librarian.

### Key tasks of the storage administrator

- Determines backup, restore and data-recovery strategies
- Puts in place adequate backup, restore and recovery procedures and makes sure these are followed
- Creates and updates all backup documentation
- Ensures that storage resources are accurate in the configuration management database (CMDB)
- Executes end-user backup and restoration requests
- Forecasts future storage capacity requirements

The storage administrator – who carries out most of the Storage Management activities and is also responsible for all of the function improvements – may be the network manager, senior technician or supplier.

### Key tasks of the media librarian

- Ensures supply and control of limited-use media (magnetic tapes, diskettes, CD-ROMs and so on)
- Audits the physical media library, and ensures consistency of logical and physical media
- Arranges for media to be stored off site in accordance with media retention and rotation policies
- Loads and removes media for backups and restores
- Logs and tracks all media in the logical media library
- Supplies and controls media for Storage Management strategy testing
- Ensures that media associated with any new service release is available

The media librarian – who maintains the media library – may be the service desk administrator or technician.

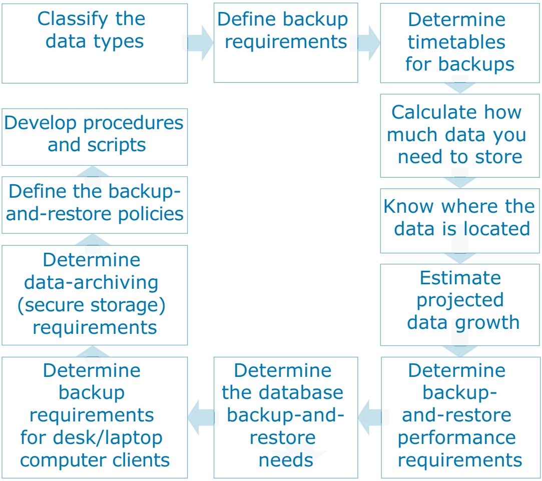
## Implement Storage Management

To implement Storage Management successfully at your school, you must first define and agree your policies and select the appropriate storage technology. In defining the Storage Management policies, there are two aspects to consider: the backup/restore strategy and storage resource management (SRM).

### 1 The backup/restore strategy

Backup, restore and data-recovery operations are some of the most important tasks in technical support. Schools cannot risk losing access to data for any significant amount of time, so you should develop and follow a carefully thought-out plan, commonly called a backup strategy.

A backup-and-restore strategy is usually developed through these steps:



Classify the data types
Define backup requirements
Determine timetables for backups
Calculate how much data you need to store
Know where the data is located
Estimate projected data growth
Determine backup-and-restore performance requirements
Determine the database backup-and-restore needs
Determine backup requirements for desk/laptop computer clients
Determine data-archiving (secure storage) requirements
Define the backup-and-restore policies
Develop procedures and scripts

You will find a detailed explanation of these steps in the Storage Management implementation guide **[http://becta.org.uk/fitsom]**.

## 2 Storage resource management

Whether the network is in one location or spread across multiple locations, you still have to manage the various storage technologies in use. This means making good use of the vendor tools that come with the various storage systems or using third-party tools that meet the school's needs. The key to success is to have well defined policies and procedures to support these technologies.

Storage resource management is a key Storage Management activity focused on ensuring that important storage devices such as disks are formatted and installed with the appropriate file systems. In addition, storage resource management includes using management technologies to monitor storage resources so that they meet availability, capacity and performance requirements.

There are two main activities in storage resource management: storage event monitoring and media management.

### Storage event monitoring

It is important to monitor storage device availability, performance and capacities regularly in order to capture the information required to analyse potential problems, performance issues or capacity shortages. This means that technical support staff must monitor all storage management events.

The basic types of event that are of interest to a storage administrator are:

- Availability – is the storage system available as it is required?
- Errors – how many hardware, software and network errors are occurring on storage systems?
- Performance – what is the performance of the storage management system?
- Capacity – which storage systems are approaching full capacity?

### Media management

Media management plays an important role in the Storage Management function and includes the various tasks associated with administering and maintaining storage media (the physical media on which data is stored).

There are two activities in media management:

- General media management – which involves managing the different types of media used in the school such as hard disks, CD-ROMs, video, audio and tape media of different sorts (for example, DAT)
- Disk management – which involves administering and maintaining both the physical disks themselves and also logical disk volumes that may be used for data storage.

## Storage technology options

Once you have defined the storage management policies, you will need to choose the appropriate backup technology. There are a number of backup technologies available to schools which range in cost from a few hundred to a few thousand pounds. The cost of each often provides an indication of the capacity, speed and ease of accessing the data on the media.

For example a Zip drive may cost about £150, have a capacity of 200MB and be slow to perform backup-and-restores. Digital linear tape (DLT) drives may cost about £3,000, have a capacity of 80GB and be very fast and reliable to perform backup-and-restores.

The Storage Management implementation guide includes a table with more information on backup technologies, with their approximate costs and the relative pros and cons of each **[http://becta.org.uk/fitsom]**.

## Implement the Storage Management policies

Follow these steps to implement the Storage Management policies.

### Prepare to implement

- Identify roles and responsibilities
- Train all staff involved in the function
- Set a start date
- Communicate plans and schedules to the implementation team
- Acquire materials for the function such as drives, media and schedules

### Assign roles and responsibilities

- Storage administrator
- Media librarian

### Install the storage solution

- Install the storage solution and the monitoring and management tools using FITS Change Management and Release Management

### Pilot the backup strategies and storage resource management

- Test backup procedures
- Test restore and recovery procedures

### Review the pilot

- Was the pilot successful?
- Apply any changes to the policies before going for full implementation

### Implement

- Hold a formal school launch to ensure enforcement
- Begin to perform the Storage Management function

## Operate Storage Management

You should set up a schedule listing all the Storage Management activities. Any errors discovered during routine backup/restore tasks should be reported as incidents to the service desk so that you keep records of their detection, diagnosis and resolution.

The following is a rough guide to appropriate timings for general activities.

### Daily

- Perform daily backup routines and update logs
- Monitor storage resources (errors, performance, capacity etc)

### Weekly

- Perform weekly backup routines and update logs
- Store archival material in secure storage
- Remove unused temporary files and user profiles
- Defragment the disk drives that hold frequently modified data

- Clean heads on tape drives and prepare media for the backups due next week
- Review the monitoring of storage resources

### Monthly

- Perform monthly backup routines and update logs
- Store archive materials in secure storage

### Periodically

- Audit the media library
- Retire ageing backup media
- Test a backup and make sure it can be restored
- Re-tension any tape cartridges used for backup

### Annually

- Review the backup schedule
- Examine incidents that required restores of data
- Consider the cost effectiveness of your storage management strategies
- Review Storage Management policies
- Rewrite and publish updated policies

# Directory Services Administration

The goal of Directory Services Administration is to set up and administer the directory services on the school's network. Directory services are to a school network what a telephone directory is to the telephone system. They store information such as names of users, computers and so on as objects with descriptive attributes. People can use the service to look up objects by name or to look up services (eg curriculum applications). In other words, directory services are simply a database of services available on the school network.

## Why have Directory Services Administration?

Directory services store information in a central place, which enables users, computers and applications to communicate across the network. This information may include computer (host) names and addresses, user names, passwords, access permissions, group membership, printers and so on.

Naming services are fundamental to any computing network. Without a central naming service, each computer would have to maintain its own copy of all this information. Naming service information can be stored in files, maps or database tables. Centralising all data makes administration easier.

## Roles and responsibilities

There are two roles in Directory Services Administration: directory designer and directory administrator.

**Key tasks of the directory designer**

- Designs the directory infrastructure to meet the school's needs
- Creates the directory database architecture
- Creates a list of changes required to an existing database schema in order to meet the new requirements of the school
- Determines the correct setup of the network infrastructure in order to ensure data replication
- Checks that replication has happened when required

The directory designer – who is responsible for creating a design that enables the directory to provide the correct information where it is needed – may be the network manager, senior technician or supplier.

**Key tasks of the directory administrator**

- Determines all directory administration, integration and operation strategies
- Ensures that applications do not conflict
- Keeps school directory documentation accurate
- Represents all directory resources in the CMDB
- Creates new directory objects and manages directory database architecture
- Monitors data replication to ensure that it occurs in a timely fashion
- Monitors the directory for capacity, availability and performance

The directory administrator – who has end-to-end responsibility for the Directory Services Administration function, and is also responsible for all of the function improvements – may be the network manager, senior technician or supplier.

# Implement Directory Services Administration

## 1 Choose your directory services structure

Very few network managers have the opportunity to implement a new school network from scratch. Directory Services Administration therefore focuses mainly on documenting, integrating and improving the existing directory to make it easy for users to access network resources and for you to add additional functionality (such as authentication and authorisation).

Many schools create their directory using the department structure or building layout of the school – for example one of the following, which helps to relate real network components to their physical location:

- School/Curriculum Department/Subject
- School/Building/Classroom.

Before you start, you need to know what you have and to understand the integration challenges.

### Know what you have

Before you can gain any positive or meaningful control over a directory, you must first know:

- What you have and how it works
- What operating systems interoperate with the other components, systems or applications
- Who has responsibility for which operating system (internal or external support).

So before you begin, document where you are today.

### Directory integration challenges

With the introduction of many disparate general and special-purpose directories, the task of managing them has become a problem. Managing disparate directories is expensive, unnecessary and not good practice.

## 2 Understand the directory environment

Before you create any policies for directory services and set the directory architecture, you will need detailed information on:

- Where directory servers and components are located on the network
- How data flows, physically and logically, through the directory
- All processes and programs running in support of the directory services
- All hardware running in support of the directory services.

Understanding the logical flow of data through a directory (the processes, applications, automation tools and so on) is just as important as understanding the physical design (where servers are located on the network). If you do not know exactly how the directory will work, both logically and physically, you will not be able to monitor proactively for performance, integrity and reliability. Also, you will not be able to troubleshoot accurately when you experience problems.

## 3 Define the Directory Services Administration policies

The school should agree, document and publish a series of policies that will form guidance for the day-to-day operation of the directory service. You will usually review these policies annually, based on performance over the previous year and the changing needs of the school.

To begin to understand what directory services policies are required, you need to categorise the use of directories into three primary areas:

- Authentication and authorisation
- Naming and locating of directory resources
- Administration and management of directory resources.

### Authentication and authorisation

Directory and security services are becoming distinct components within the network services model. Still, these two services are inextricably linked, providing authentication and authorisation functions. Security and directory services operate in tandem. Initially, the directory must provide authentication and access controls that govern who can access and modify the directory.

### Naming and locating network resources

The directory's core competency and traditional role is to find things. Naming and locating network resources on the network is a significant role that directories play.

### Administering and managing network resources

A number of activities need to be carried out to keep the network resources reliable and available. These activities include administering the network addresses, which is part of the FITS OM Directory Services Administration function, and equipment maintenance, which is part of the FITS Availability and Capacity Management process.

## Implement the Directory Services Administration policies

Follow these steps to implement the Directory Services Administration policies.

### Prepare to implement

- Identify roles and responsibilities

- Train all staff involved in the function
- Set a start date
- Communicate plans and schedules to the implementation team
- Acquire materials for the function, such as software

**Assign roles and responsibilities**

- Directory designer
- Directory administrator

**Install and pilot the Directory Services Administration policies**

- Pilot the new directory on a separate test network
- In the absence of a test network, pilot the new directory on the live school network at a time when users do not need access to network resources
- Install the new directory services using FITS Change Management and Release Management

**Review the pilot**

- Review the pilot based on monitoring, results of test scripts and the content of log files and reports
- Apply any changes to the policies before going for full implementation

**Document the directory**

- Document the directory fully and enter it into CMDB
- Make all future changes to the directory under the Change Management process

**Implement**

- Hold a formal school launch to ensure enforcement
- Begin to perform the Directory Services Administration function

## Operational aspects of Directory Services Administration

### Monitoring your directory

By monitoring the directory, you can spot outages as soon as they occur and even, in some cases, before they occur. With more sophisticated monitoring tools, you can further anticipate failures, understand where performance degradation exists and capture this information for the purpose of system tuning.

### Maintaining your directory

The data held in the directory is critical to the operation and teaching capability of your school. If the directory becomes unavailable for any reason (for example through equipment failure or data corruption), the school will suffer.

Developing sound backup-and-restore procedures for the directory and supporting system components should mean that you do not lose critical directory data or configuration information. The development of the backup-and-restore procedures themselves is equally important. Simply having a backup process is not enough. You also need a clear, concise and thoroughly executable restore plan that the individuals responsible for the process test regularly. If you have to carry out restores without a plan, you will find yourself exposed to data loss and/or significant system downtime.

The Storage Management function covers all aspects of backup-and-restore strategies. When you are making changes to the directory service, always use the Change Management process in support of the change.

### Managing your directory

Managing directory services is all about knowing exactly what is in place, what it is doing and how well it is performing the functions for which it was deployed.

The kinds of activities that will be involved in the day-to-day management of directory services include:

- Creating, deleting, moving or editing attributes
- Security
- Replicating databases (if more than one domain is in use on your network).

These activities usually depend on the software you use to manage and maintain your directory, so you should refer to the vendor's documentation for detailed guidance.

**Troubleshooting the directory**

From time to time during a directory's lifetime, things will go wrong. Based on the type and severity of the fault, your school may experience anything from slight degradations in performance to full failure of the directory service. When something does go wrong, your objectives are to minimise the damage, return the directory to full service as quickly as possible and understand the fault so that you can take steps to prevent its recurrence.

Directory faults can be broken down into three categories:

- Outages resulting from hardware or software failures
- Performance problems
- Problems with directory data.

Any directory services incident that occurs should be reported to the service desk to ensure that it is logged and any affected users notified about it. You should then use Incident Management to restore the services with a workaround or refer to Problem Management to put in place a permanent fix.

You will find a more detailed explanation, plus a flowchart and checklist for troubleshooting the directory, in the Directory Services Administration operations guide **[http://becta.org.uk/fitsom]**.

## Operate Directory Services Administration

Your Directory Services Administration tasks will be determined by the type and quantity of data. The following list is a rough guide to appropriate timings for general activities.

### Daily

- Monitor the directory
- Back up the directory

### Weekly

- Review attempts to access unauthorised resources
- Review backup logs

### Monthly

- Review performance of the directory service

### Periodically

- Review the structure of the directory service
- Check whether the structure is still applicable – for example, if staff move offices

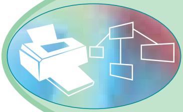
### Annually

Review the whole Directory Services Administration policies to check:

- Whether they have hit the targets in any service level agreements in place
- Whether the policy is still appropriate for your school.

In addition, you will need to cater for directories for incoming and outgoing students.

# Print and Output Management



The goal of Print and Output Management is to ensure that all printed and electronic material is produced in the most efficient and cost-effective manner, using the most appropriate hardware and software available.

Print and Output Management is concerned with the design, implementation, security and management of output in order to meet the school's requirements.

## Why have Print and Output Management?

All schools create some form of output. Examples of ICT output include faxes, emails, web pages, electronic transactions and computer files. However, the most common form of output is the printed page.

Effective operational management of the print and output devices keeps costs under control and makes appropriate resources available to the school for teaching, learning and management.

Using proactive Print and Output Management will increase the reliability of printing devices and the speed of producing or distributing important output. The time invested in implementing and operating Print and Output Management will therefore result in increased efficiency for staff and students.

## Roles and responsibilities

There are three roles in Print and Output Management: network manager, print administrator and print support technician.

### Key tasks of the network manager

- Develops the print and output policies and maintain controls and procedures
- Drives the efficiency and effectiveness of the function
- Monitors school-critical outputs to ensure compliance with agreed service levels
- Understands the needs of the users and the school

The network manager – who sets up and manages the function – may be the network manager or a supplier.

### Key tasks of the print administrator

- Creates printer standards to minimise spare parts
- Manages the acquisition, retiring, repair, configuration and location of printers
- Represents printing assets in the CMDB
- Manages the creation and distribution of reports which are the responsibility of technical support
- Manages the storage, retention and destruction of paper and software archives

The print administrator – who is responsible for installing and configuring printing hardware and output software – may be the network manager, the senior technician or a supplier.

### Key tasks of the print support technician

- Handles service requests
- Investigates, diagnoses and resolves incidents
- Raises a record and notifies the problem manager when a problem is identified

The print support technician – who is responsible for troubleshooting and repairing printers, print queues etc whenever an incident occurs – may be the technician or a supplier.

## Implement Print and Output Management

To implement Print and Output Management successfully at your school, you must first define and agree your policies and select the appropriate printing technology. To define the Print and Output Management policies, you will need to consider these six main aspects.

### 1 General design policies

General design policies are based on the overall requirements of the school. You first need to ascertain the requirements by considering these points:

- What output each department requires
- The volume of output required
- Mix of hard-copy printing and software-based output
- The approach to printer management
- How consumables are paid for
- The use of quotas
- The finish required for printed output
- Security requirements for departments.

You will find a print/output requirements template to help you gather the information in the Print and Output Management toolkit **[http://becta.org.uk/fitsom]**.

### 2 Locating printers

Most users need to know the physical location of printers. Printers should be placed close to the people who are using them, but they also need to be near the print server or computer they are connected to on your network. Another consideration should be to minimise the impact of printing on the performance of the network. Check the network infrastructure design and try to prevent print jobs from hopping through multiple inter-network devices. In addition, you may want to isolate any group of users who have high-volume printing needs with their own printer on their segment of the network in order to minimise the effect on other users.

## 3 Print and Output Management standards

The use of standards means less complexity and reduces support costs. This in turn can lead to increased productivity and lower ongoing costs. Standards to consider are:

- Relationship between the size of document and speed of printer
- Limits on the size of print jobs sent to each printer
- Limits on the size of print jobs sent by each user
- Limits to the available destinations for each user
- Dedicated printers for school-critical output
- Spooling for jobs to be suspended, deleted, moved and reprinted.

## 4 Printer-naming considerations

Establish a printer-naming strategy for the school, as too many names for the same devices can lead to confusion.

- The printer itself can usually store a name.
- The network may also have a name for the printer.
- Each computer referencing that printer will have a name for the printer.
- Even applications may have their own names for the printer.

Make sure you develop a naming strategy that makes sense and is easy to use, and then implement it in line with Directory Services Administration.

## 5 Document retention

Retention is about how long to keep documents in the repository. The document life-cycle concept implies that a document is useful for a specific time period. Both legal and school requirements may influence this decision, with legal requirements sometimes taking precedence. When we talk about a document repository, we mean somewhere where we store print and output documents, so it could be a filing cabinet, a fire safe or a central server holding email documents.

## 6 Supplies replenishment

Printers have a habit of consuming lots of paper, toner and ink. Your school must decide how to handle the management and replenishment of these supplies: you will have to think about both the physical replenishment and the ordering process. There are two options for this: central management and distributed management.

The supplies management policy should also include recycling. Toner and ink cartridges as well as other media are recyclable – and recycling's good for the planet!

# Printing technology options

### Types of printer

There is a variety of printing technologies suitable for use in a school environment. Printer prices vary widely since speed, quality of build and the numbers of pages produced between maintenance intervals (the duty cycle) all have a significant impact on the costs.

The Print and Output Management implementation guide provides a table with more information on types of printing technologies, how they work and the approximate costs of each **[http://becta.org.uk/fitsom]**.

### Electronic output

There are two main considerations for electronic output: electronic format and electronic output distribution.

The Print and Output Management implementation guide contains further details on these **[http://becta.org.uk/fitsom]**.

## Implement the Print and Output policies

Follow these steps to implement the Print and Output Management policies.

### Prepare to implement

- Identify roles and responsibilities
- Train all staff involved in the function
- Set a start date
- Communicate plans and schedules to the implementation team
- Acquire materials for the function such as hardware, drivers, output software, consumables and schedules

### Assign roles and responsibilities

- Network manager
- Print administrator
- Print support technician

### Install the print and output solution

- Install the print and output solution, and the monitoring and management tools, using FITS Change Management and Release Management

### Pilot the print and output policies

- Test new output mechanisms such as internet, intranet, PDF

### Review the pilot

- Was the pilot successful?
- Apply any changes to the policies before going for full implementation

### Implement

- Hold a formal school launch to ensure enforcement
- Begin to perform the Print and Output Management function

## Operate Print and Output Management

Set up a schedule listing all the Print and Output Management activities. Any errors discovered during routine maintenance tasks should be reported as incidents to the service desk so that you keep records of their detection, diagnosis and resolution.

You will need to define and document schedules for these activities.

### Daily

- Load paper and clear any paper jams
- Replace toner and ink cartridges
- Cancel, move, restart or end print jobs that have failed

### Weekly

- Carry out maintenance tasks as described in the device's user manual
- Delete temporary files created from soft-copy output
- Check for and purge any documents whose retention period has expired
- Review paper, toner and ink supplies

### Monthly

- Review print quotas
- Use and review charge-back system (if in place)

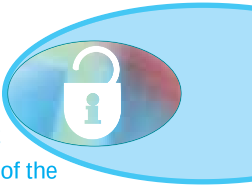
### Periodically

- Service printers/fax machines
- Review email/disk quotas
- Update drivers and firmware

### Annually

- Review Print and Output Management policies
- Rewrite and publish updated policies

# Security Administration



The goal of Security Administration is to maintain a safe computing environment in a school. Security is an important part of the school network: an information system with a weak security foundation will eventually experience a security breach that will result in the loss of confidentiality, integrity and availability of the data.

In addition, Security Administration takes into account the physical security of the network. This involves issues such as access to the server room, security of individual computers and security policies for accessing the internet.

## Why have Security Administration?

Security Administration is concerned with all aspects of security necessary for maintaining a safe and secure computing environment:

- Personnel security – clearing users to handle the data that they access
- Application security – making critical applications secure from unauthorised access
- Operating system security – ensuring that systems and services dependent on the operating system cannot be compromised
- Hardware security – protecting hardware assets both inside and outside the school
- Network security – protecting data held on the network from unauthorised viewing and tampering
- Physical security – limiting physical access to computer systems to authorised personnel only.

## Roles and responsibilities

There are two roles in Security Administration: security administrator and security support technician.

### Key tasks of the security administrator

- Provides effective network domain security design and management
- Tests and implements strategic security technology
- Monitors network and third-party vulnerability
- Manages authentication and access method requirements
- Manages user policy usage and requirements
- Performs audit tracking and reporting
- Detects intrusions and protects against viruses
- Provides ongoing technical support and subject matter expertise for security initiatives in the school

The security administrator – who is the owner of the Security Administration function and is also responsible for all the function improvements – may be the network manager, the senior technician or a supplier.

### Key tasks of the security support technician

- Adds, deletes and changes user accounts
- Ensures that passwords conform with school policy
- Checks that encrypted file systems follow the standard
- Ensures that only authorised personnel gain physical access to the building and computer assets
- Performs periodic audits of network environment and security
- Maintains up-to-date antivirus/spyware software

The security support technician may be the technician or the service desk administrator.

## Implement Security Administration

To implement Security Administration successfully at your school, you must first define and agree your policies and select the appropriate security technology. To define the Security Administration policies, you will need to carry out the following six main activities.

### 1 Asset and data classification

All school network assets (hardware, software and data) must be made secure to a certain extent. To determine the amount of security applied to an asset, you first have to classify it. Activities within asset and data classification include:

- Hardware and software classification
- School data classification
- Security risk assessment.

### 2 Identification

Identification is the mechanism by which the system asks the user, "Who are you?" Users identify themselves to the system by means of a user ID (also referred to as a user name or logon name). User IDs must be unique so that no two users in a system have the same user ID. To ensure that user IDs are unique, it is important to develop a logon-naming standard that clearly addresses all name characteristics.

A well-defined naming convention has the following characteristics:

- User IDs are easy for users to remember (for instance paul.stonier)
- User IDs are easy for administrators to create
- Administrators can easily determine the owner of any user ID.

## 3 Authentication

Authentication is the mechanism by which the system asks the user, "Is that **really** you?" If a system has a good logon naming standard, but no authentication, then anyone could log on to the system by using someone else's account, since it may be possible to guess user IDs. To make sure that only the true owner can get into the account, the system must therefore enforce some sort of authentication mechanism. This usually makes use of a password or personal identification number (PIN).

A good password that provides a high level of security has the following characteristics:

- Is alphanumeric and at least eight characters long
- Has at least two letters, one number and one special character
- Does not use proper names
- Uses a mixture of lower- and upper-case letters
- Appears random and is changed at least every 60–90 days
- Is not reused for six months and is different from the previous passwords.

## 4 Access control and authorisation

Access control provides a mechanism for setting up new users (or for giving existing users additional privileges or restrictions). There are two equally important processes: one allows users to access services and the second one removes them. Removing redundant and unused user IDs is essential, as these constitute additional security risks to the school network.

You will find access control templates for new and leaving users in the Security Administration toolkit **[http://becta.org.uk/fitsom]**.

Once users have been authorised to access the school network, they can access the services they require. Most student users, however, have only limited access to the network.

Authorisation is the mechanism by which user access is determined. User access must always follow the 'least privilege' principle, which means that users may have the access required to perform their required functions and no more. Technical support staff, on the other hand, should have full access to the network.

## 5 Hardware security

Your school needs a policy for looking after the valuable hardware components of your network. When you mention hardware security, most people think first and foremost about the theft of school computers or peripherals. This is a real risk, and many schools use mechanisms for locking PCs to desks to deter thieves.

Hardware security takes this a little further, however, and a school's hardware security policy should include the following:

- Securing access to the school's servers
- Protecting critical hardware by means of uninterruptible power supplies and failover systems for servers
- Securing backup media
- Securing sensitive output documentation (whether from a printer or as a PDF file)
- Keeping copies of all security keys and associated documentation.

## 6 Control and audit

Control and audit deals with ongoing safety checks of all school assets under Security Administration, and needs to be considered with physical audits and software/data events.

For physical audits, audit all school network assets regularly as prescribed by FITS Configuration Management and, if a CI is missing, raise an incident report with the service desk.

With software/data events, regular analysis on audit log files enables the security administrator to track and maintain an adequate level of security, and, if an unusual event occurs, raise an incident with the service desk.

### Security technology options

There are three security technology options to consider: using encryption software, securing the hardware and perimeter monitoring.

#### Encryption software

If files and data in school require encryption, the operating systems you utilise ought to be able to provide the necessary encryption. You could use ICT security software such as IPsec, which encrypts all IP traffic and guarantees that the source of the data and the recipients are genuine.

#### Securing hardware

You can use padlocks or equivalent controls to protect workstations, peripherals and laptop computers physically. In addition, various mechanisms are readily available for securing servers in cupboards or a server room, whether 'lock and key' or the various combination-type locks on the market.

### Perimeter monitoring

A school with a number of computer suites available to students and staff all day would find it impossible to monitor all its hardware from a physical and practical point of view. Closed-circuit television (CCTV) is becoming a relatively inexpensive technology and can provide a significant continuous security deterrent.

## Implement the Security Administration policies

Follow these steps to implement the Security Administration policies.

### Prepare to implement

- Identify roles and responsibilities
- Train all staff involved in the function
- Set a start date
- Communicate plans and schedules to the implementation team
- Acquire materials for the function such as forms, technology and schedules

### Assign roles and responsibilities

- Security administrator
- Security support technician

### Install the security solution

- Install the security solutions, monitoring and management tools using FITS Change Management and Release Management

### Pilot the Security Administration policies

- Test the creation of user profiles and groups
- Test encryption software, auditing, security logs and so on

### Review the pilot

- Was the pilot successful?
- Apply any changes to the policies before going for full implementation

### Implement

- Hold a formal school launch to ensure enforcement
- Begin to perform the Security Administration function

## Operate Security Administration

Set up a schedule listing all the Security Administration activities. Any security incidents should be reported to the service desk so that you keep records of their detection, diagnosis and resolution. Any changes to security policies or technology must be reflected in the security schedule.

The following is a rough guide to appropriate timings for general activities.

### Daily

- Audit software/data logs and check for security breaches
- Raise incident reports for any potential security breaches
- Administer user accounts and passwords

### Weekly

- Check the security of hardware assets
- Check locks to cupboards and server rooms
- Check that all keys and their documentation are secure

### Monthly

- Sample a small number of user accounts to confirm that their passwords comply with school policy

### Periodically

- Audit all hardware components of the school network against the CMDB

### Annually

- Review Security Administration policies
- Rewrite and publish updated policies

# Patch Management

The goal of Patch Management is to keep the components installed on the network (hardware, software and services) up to date with the latest patches and updates. The network components covered in Patch Management may include computers, servers, software, peripherals, cabling, routers and switches, plus services such as messaging, database, MIS and file storage.

## Why have Patch Management?

Patch Management is an important part of keeping the components of the network available to the end user. Without regular patching, your ICT infrastructure could fall foul of problems which are fixed by updating regularly the software, firmware and drivers. Poor patching can also allow viruses and spyware to infect the network. Patch Management should be a centralised, managed service that guarantees protection, rather than a user-installed, piecemeal approach that leaves you uncertain about the overall state of the network.

Protecting the network with security measures provides one layer of protection, and educating your users about the threats of spyware and malware provides another layer. Users need to know what to do when they receive an email from an unknown source: whether just to delete it, report it to technical support or open it. Users also need to know how to deal with browser plug-ins or instructions from browsers to ‘click here to install updates’, as these could easily be spyware attempts to infect that computer. It is possible to counter threats like these with a combination of software and user education.

## Roles and responsibilities

There is one role in Patch Management: the patch administrator.

The patch administrator, as the owner of the Patch Management function, is responsible for all of the function improvements. As Patch Management works closely with Security Administration and FITS Change Management and Release Management, you can combine some of the roles – which may be performed by the network manager, a senior technician or a supplier.

### Key tasks of the patch administrator

- Ensures that all operating systems and software have up-to-date service packs and patches
- Keeps drivers up to date
- Keeps firmware up to date
- Keeps antivirus and antispyware definitions up to date
- Produces Release Management build procedures for major updates to enable other technicians to carry out the updates
- Checks that installations of patches and updates are successful

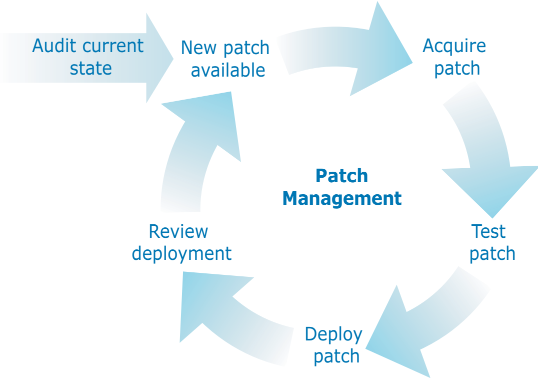
The patch administrator must keep informed about the release of new updates, drivers, patches and firmware. This may take up considerable time unless the task can be automated (for instance, by email notifications from vendors and manufacturers).

## Implement Patch Management

To implement Patch Management successfully at your school, you must first define and agree your policies and then follow the patch management cycle. When defining the Patch Management policy, you may want to include the following:

- A list of computers, servers and peripherals on the network covered under the policy (this information should be available in your CMDB)
- Allocation of roles and responsibilities for Patch Management activities
- Patch Management schedules
- A list of which patches and updates will be carried out using the FITS Change Management and Release Management processes, and which may be done without them
- Definitions of which email attachments and internet downloads are safe to open and how this will be communicated the users.

## The Patch Management cycle



As the diagram shows, there are six steps in the Patch Management cycle.

## 1 Audit current state

Before you can maintain your network, you need to understand its current state. This involves identifying the hardware, software, operating systems applications and their patch levels. Other hardware and peripherals such as printers and switches have firmware that you should also identify.

If you do not have all this information to hand either in a CMDB or on lists or spreadsheets, this may seem a big job to start with. However, the information is vital for successful Patch Management implementation.

Your CMDB will contain information about each hardware and software component, known in FITS as a configuration item (CI), installed on the network. For Patch Management it is recommended that you also keep the following attribute information for each CI:

- Computer – BIOS, firmware, systems board, video and network drivers
- Operating system – service and feature packs, patches
- Switch – firmware
- Antivirus – data file/virus definition update
- Antispyware – data file/spyware definition update
- Printer and scanner – driver, firmware.

Once you know the current state of your network, you can begin to plan to bring it up to date by installing the latest drivers, patches, firmware and definitions. The aim of bringing everything up to date is to create a baseline from which you can start regular patch maintenance, as the process is far easier if everything is at the same level to begin with.

## 2 New patch available

News that a new patch is available may come from a variety of sources such as manufacturers' websites, suppliers' bulletins or technical forums. The patch will usually have some release information explaining what the patch fixes and who should use it. Read the information carefully and ensure that the patch applies to the components and overall network structure of your school. The patch may not be applicable to every component on the network, in which case you need to identify which components require the patch.

## 3 Acquire patch

The next step is to acquire the patch by downloading it from the internet, getting it sent by post or having it emailed to you. Some of the new service packs are hundreds of megabytes in size, in which case requesting those on CD will save you bandwidth and download time.

## 4 Test patch

Test the patch on a computer or other device reserved for testing (or a limited number of live computers). The testing itself depends on what the patch claims to fix. You may be able to ascertain that the bug has been fixed, although most patches nowadays are for obscure security holes. Once you are satisfied that the computer or other device still works properly and that the patch has not created other faults, continue to the next step.

## 5 Deploy patch

This step may involve imaging a computer and deploying the new image, or it may involve visiting every computer affected by the patch. Again, this depends on the tools you have available and the patch management strategy you employ.

Installing the latest drivers, patches and updates on every computer in school can obviously take a lot of time and may seem like an endless task. However, you can speed up the process by using software deployment tools. Tools such as disk imaging or patch management software, along with antivirus administration console software, can help make the task less burdensome.

Disk imaging is one method of bringing several computers up to date reasonably quickly. Using Release Management you should be able to document and prepare an image in a consistent way, and then use the Change Management process to deploy the image.

### 6 Review deployment

Once you have deployed the patch, check that none of the computers with the new patch is adversely affected. Also, you need to check that the patch is installed successfully. You cannot assume that the patch has been installed on every computer, as other factors such as lack of disk space, computer shutdown or network problems may have affected the deployment.

Once you have ascertained that the patch has been deployed successfully, update the CMDB and/or the request for change document associated with this change. Report any incident or problem to the service desk for resolution using Incident Management or Problem Management.

## Implement the Patch Management policies

Follow these steps to implement the Patch Management policies.

### Prepare to implement

- Identify roles and responsibilities
- Train all staff involved in the function

- Set a start date
- Communicate plans and schedules to the implementation team
- Acquire materials for the function such as CMDB, automating tools and schedules

**Assign roles and responsibilities**

- Patch administrator

**Install the patch management solution**

- Install the automating, monitoring and management tools using FITS Change Management and Release Management

**Pilot the Patch Management policies**

- Test the automating tools
- Test the changes on a small group of computers

**Review the pilot**

- Was the pilot successful?
- Apply any changes to the policies before going for full implementation

**Implement**

- Hold a formal school launch to ensure enforcement
- Begin to perform the Patch Management function

## Operate Patch Management

Set up a schedule listing all the Patch Management activities. Any incidents related to the deployment of patches should be reported to the service desk so that you keep records of their detection, diagnosis and resolution. Any changes to patch management policies or technology must be reflected in the patch schedule.

The following is a rough guide to appropriate timings for general activities.

### Weekly

- Check for new software patches
- Check the latest antivirus and spyware definitions
- Check for news about new threats, patches and releases

### Monthly

- Check that drivers (for example video and network) are up to date
- Check antivirus engine updates

### Periodically

- Check for new printer drivers
- Check computer and server BIOS firmware

### Annually

- Check for new operating system versions
- Check for new switch, hub and router firmware

# Further guidance

This FITS OM pocket guide is part of our series of ICT Technical Support products.

## Resources available

- FITS – online and downloadable
- FITS pocket guide
- FITS assessment
- FITS expert workshops
- FITS evaluation report and summary sheet
- FITS case studies
- FITS OM – online and downloadable
- FITS OM assessment

## Resources under development

- Primary FITS
- FITS for FE
- ICT workforce management

## For the latest FITS news

If you would like to keep abreast of our latest developments, you can register to receive updates **[http://becta.org.uk/fits]**.

## FITS OM downloads

**FITS OM Introduction**

(last updated February 2006 – PDF 496KB)

**Systems Administration**

(last updated February 2006 – PDF 498KB)

**Storage Management**

(last updated February 2006 – PDF 1.4MB)

**Directory Services Administration**
(last updated February 2006 – PDF 1.1MB)

**Print and Output Management**
(last updated February 2006 – PDF 1.2MB)

**Security Administration**
(last updated February 2006 – PDF 1.8MB)

**Patch Management**
(last updated February 2006 – PDF 1.0MB)

## Overview of Becta

Becta is the Government's lead partner in the strategic development and delivery of its e-strategy for the schools and the learning and skills sectors.

Publication date: October 2006

While great care has been taken to ensure that the information in this publication is accurate at the time of publication, we accept no responsibility for any errors or omissions. Where a specific product is referred to in this publication, no recommendation or endorsement of that product by Becta is intended, nor should it be inferred.

Becta
British Educational Communications
and Technology Agency

Millburn Hill Road
Science Park
Coventry
CV4 7JJ

Tel: 024 7641 6994
Web: http://www.becta.org.uk

**FITS OM (Framework for ICT Technical Support Operations Management)**

**email:** fits@becta.org.uk
**Web:** http://www.becta.org.uk/schools/technicalsupport

10/DD06-07/074/PC/3K