Problem Management

Problem Management Contents

Key

Glossary term:	Glossary term
Cross reference:	Cross reference

Becta

ICT Advice

Problem Management

Publication date March 2004

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

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

Becta
ICT Advice

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

Problem Management

PrM 1 Introduction to Problem Management

You have the same problem occurring time after time with your ICT and it never gets fixed properly? You need the FITS Problem Management process.

PrM 1.1 Aim

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

PrM 1.2 Objectives

The objectives of this section are to enable you to:

- understand the difference between incidents and problems
- understand when a quick fix is not enough to resolve a problem permanently
- decide whether you need to implement problem control
- understand how to implement the Problem Management process
- understand how to achieve workarounds and solutions
- decide which Problem Management reports your school requires and how to produce them.

PrM 2 Overview

PrM 2.1 What is Problem Management?

The goal of Problem Management is to minimise both the number and severity of incidents and problems in your school. It should aim to reduce the adverse impact of incidents and problems that are caused by errors in the ICT infrastructure, and to prevent recurrence of incidents related to these errors.

- You should address problems in priority order, paying attention to the resolution of problems that can cause serious disruption.
- The degree of management and planning required is greater than that needed for incident control, where the objective is restoration of normal service as quickly as possible.
- The function of Problem Management is to ensure that incident information is documented in such a way that it is readily available to all technical support staff.

Problem Management has reactive and proactive aspects:

- reactive – problem solving when one or more incidents occur
- proactive – identifying and solving problems and known errors before incidents occur in the first place.

Problem Management includes:

- problem control, which includes advice on the best workaround available for that problem
- error control.

PrM 2.1.1 Differences between incident management and problem management

- The aim of incident management is to restore the service to the customer as quickly as possible, often through a workaround, rather than through trying to find a permanent solution.
- Problem management differs from incident management in that its main goal is the detection of the underlying causes of an incident and the best resolution and prevention.
- In many situations the goals of problem management can be in direct conflict with the goals of incident management.
- Deciding which approach to take requires careful consideration. A sensible approach would be to restore the service as quickly as possible (incident management), but ensuring that all details are recorded. This will enable problem management to continue once a workaround had been implemented.
- Discipline is required, as the idea that the incident is fixed is likely to prevail. However, the incident may well appear again if the resolution to the problem is not found.

PrM 2.1.2 Incident vs problem

An incident is where an error occurs: something doesn't work the way it is expected. This is often referred to as:

- a fault
- error
- it doesn't work!
- a problem

but the term used with FITS is 'incident'.

A problem can be:

- the occurrence of the same incident many times
- an incident that affects many users
- the result of network diagnostics revealing that some systems are not operating in the expected way.

Therefore a problem can exist without having immediate impact on the user, whereas incidents are usually more visible and the impact on the user is more immediate.

PrM 2.1.3 Error control

Error control covers the processes involved in the successful correction of known errors. The objective is to remove equipment with known errors that affects the IT infrastructure in order to prevent the recurrence of incidents. Error control activities can be both reactive and proactive.

Reactive activities include:

- identifying known errors through incident management
- implementing a workaround.

Proactive activities include:

- finding a solution to a recurring problem
- creating a solution
- including the solution in the database of known errors.

PrM 2.1.4 Examples of problems

Technical problems can exist without impact to the user. However, if they are not spotted and dealt with before an incident occurs, they can have a major impact on the availability of the computer service.

User-experienced problems

- The printer will not form-feed paper, so users have to advance the paper by using the form-feed button.
- Each time new users log onto a computer, they have to reinstall the printer driver.
- Windows applications crash intermittently without an error message. The computer will restart and work properly afterwards.

Technical problems

- Disk space usage is erratic: sometimes there appears to be plenty of disk space, but at other times not much is available. There is no obvious reason and no impact on the users – yet!
- A network card is creating a high level of unnecessary traffic on the network. This could eventually reduce the bandwidth available, which would lead to a slow response to network requests.

PrM 2.2 Who uses Problem Management?

Problem Management is used mainly by technicians. At this stage, reference to previous incidents, a knowledge base or quick fixes will not be effective as the problem has not previously occurred. This is where the technician calls upon all their problem-solving skills and analysis techniques to decide how to approach the problem, how much time to allocate and what to do if the problem cannot be resolved.

If your school has numerous incidents that cannot be resolved readily and you are implementing lots of quick fixes, you should decide to tackle the cause of the incidents using problem management. If you get the same incident occurring repeatedly, you should implement the FITS Problem Management process.

All schools should have a process to deal with major incidents – for example, a server crash, a virus attack or an unexplained slow network. If you would like to manage your approach to major incidents, you should also consider introducing Problem Management at your school.

Most organisations, including schools, need to keep records of how well their ICT systems are functioning, what is failing and how long systems are unavailable. The information you will gain from problem management should enable you to report to the school on the technical issues that create incidents and problems. To provide your school with an effective approach to its technical support, you should always implement problem management alongside incident management.

PrM 2.3 Why use Problem Management?

The benefits of taking a formal approach to problem management include the following.

- There is a standard way to approach every problem – this saves time.
- The number of incidents will reduce.
- The solutions will be permanent. There will be a gradual reduction in the number and impact of problems and known errors, as those that are resolved will stay resolved.
- You learn from your mistakes. The process provides the historical data from which to identify trends, and the means of minimising failures and reducing the impact of failures.
- You will obtain a better first-time fix rate of incidents because you will have a knowledge database available to the service desk and technicians when a call is first logged.

PrM 2.3.1 What happens if Problem Management is not used?

Without problem management, you may observe that your school:

- faces up to problems only after the service to users has already been disrupted
- loses faith in the quality of its technical support, with high costs and low motivation for both users and technicians, since similar incidents have to be resolved repeatedly without anyone able to provide permanent solutions.

PrM 2.3.2 Objectives of recording problem management information

One function of problem management is to ensure the documenting of incident information in such a way that it is readily available to service desk staff and technicians. The information should be recorded so that it is easily referenced by simple and detectable triggers from new incidents.

Regular inspection of your problem management records can ensure the continued relevance of documentation in the light of changes in:

- technology
- available external solutions
- school practices and requirements
- in-house skills
- frequency and impact of recurring incidents
- interpretation of internal best practice.

It is important that you review your process for recording incidents and problems to enable you to make continuous improvements to the way information from previous incident resolutions is used. You may like to consider these suggestions.

- Staff using the information should be trained to understand the depth and power of the information available, how to access and interpret it, and their role in providing feedback on its relevance and ease of use.
- You should maintain a suitable spreadsheet or database for recording the information.
- Develop an integrated service management tool (see Service Desk) that can capture the information at the logging or analysis stage of the incident-handling process.

PrM 2.3.3

Benefits of problem management

The benefits of taking a formal approach to problem management include the following.

- **Improved quality of the ICT service**

  High quality reliable service is good for school leaders, teachers and students. It is also good for the productivity and morale of the technical support staff.

- **Reduction in the volume of incidents**

  Problem management helps to reduce the number of incidents that can interrupt the school day.

- **Permanent solutions**

  There will be a gradual reduction in the number and impact of problems and known errors, as those that are resolved stay resolved.

- **Improved technical support knowledge**

  The FITS Problem Management process is based on the concept of learning from experience. The process provides the historical data to identify trends, and the means of minimising failures and of reducing the impact of failures, resulting in improved productivity.

- **A more effective service desk**

  Eventually the service desk will be able to resolve a number of incidents. There will be a better first-time fix rate at the service desk as problem management enables the service desk staff to know how to deal with problems and incidents that have previously been resolved and documented.

PrM 2.3.4

What weakens the benefits of problem management?

The following can weaken the benefits of problem management.

- **Poor incident control**

  The absence of a good incident control process means that you will not have detailed historical data on incidents, which is necessary for the correct identification of problems.

- **Absence of co-ordination with incident management**

  Failure to link incident records with problem/error records means a failure to gain many of the potential benefits. This is a key feature in moving from reactive support to a more planned and proactive support approach.

- **Lack of management or leadership commitment**

  The result of lack of commitment at the top is likely to be that support staff (who are usually also involved in reactive incident control) cannot allocate enough time to structured problem-solving activities.

- **Undermining the service desk role**

  All incident reports must come through the service desk and not direct to the technician. Difficulties will arise if the service desk is dealing with multiple reports of incidents and the technician is not fully aware of the extent of the problem.

- **Not maintaining call log or incident sheets**

  Any failure to set aside time to build and update the call log or incident sheets will restrict the benefit of understanding the bigger picture on the network and looking at trends that may point towards an underlying problem.

- **Ignorance of the impact of incidents and problems**

  If you are unable to determine accurately the impact on the school of incidents and problems, you will not be in a position to give critical incidents and problems the correct priority.

PrM 2.4 How problem management works

Problem management works by using analysis techniques to identify the cause of the problem. Incident management is not usually concerned with the cause, only the cure. Problem management therefore takes longer and should be done once you have dealt with the urgent stage of the incident: for example, removing a faulty computer and replacing it with a working computer. This takes the urgency away and leaves the faulty computer ready for diagnostics.

Problem management can take time. It is important to set a time limit on how much time should be spent on the problem – or the cost of resolution can become expensive.

To achieve the goal, problem management aims to:

- identify the root cause
- initiate actions to improve and correct the situation.

PrM 2.4.1 Summary of the Problem Management process

PrM 2.4.1.1 Inputs to Problem Management

Inputs to the Problem Management process are:

- incident details from the Incident Management process
- configuration details from the configuration management database
- details about changes made to the part of the network with the problem
- any defined workarounds (from incident management).

PrM 2.4.1.2 Outputs from Problem Management

Outputs from the Problem Management process are:

- known errors
- requests for change (through change management)
- an updated problem record (including a solution and/or any available workarounds)
- for a resolved problem, a closed problem record
- knowledge base content to use in incident management
- management information through reports.

PrM 2.4.1.3 Activities of Problem Management

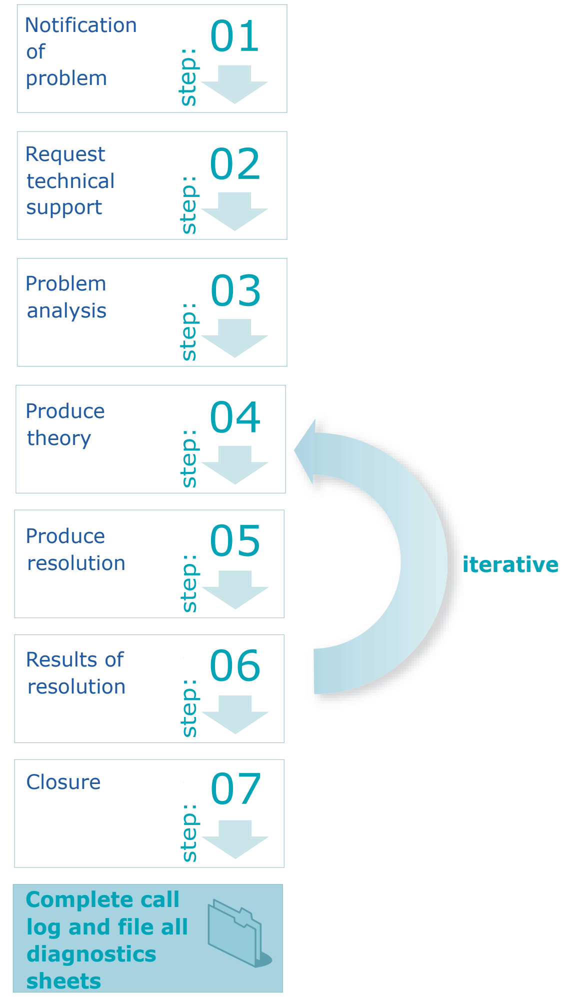
The major activities of Problem Management are:

- problem control
- error control
- the proactive prevention of problems
- identifying trends
- obtaining management information from problem management data
- the completion of major incident or problem reviews.

PrM 2.4.1.4 Roles and responsibilities in Problem Management

For an outline of the roles and responsibilities, see PrM 5.

PrM 2.4.2 Problem Management life cycle



Problem management life cycle

PrM 2.5 What does Problem Management cost?

- Initially it costs someone’s time and effort to look at problems and document an approach to resolving them in the future.
- The technician should be able to put time aside each week to look at problems. This time should be protected.

As a proactive process, problem management:

- will save time, as fewer incidents are logged
- will save budget, as the technician's salary is not used on resolving the same incident many times
- will increase the availability of equipment since it will fail less often
- will increase the confidence of the users – both teaching staff and students – as the systems become more reliable.

PrM 3 Implementation guide

PrM 3.1 Define what needs to be done to implement Problem Management

Problem Management should be implemented with Incident Management or shortly afterwards.

- Ensure that you are recording your calls and can track their progress.
- Understand the difference between problems and incidents.
- Have a procedure to separate incidents from problems.
- Decide how much time each week to devote to problem management.
- Choose which areas to improve and which of your current processes to remove.
- You need to sell the idea to other staff, so make sure you're happy with it first.

PrM 3.1.1 The Problem Management process

1. Notification of problem
2. Request for technical support
3. Problem analysis
4. Production of theory
5. Production of resolution
6. Results of resolution
7. Closure

See also the following.

- PrM 2.4.2 Problem Management life cycle
- PrM 2.1 What is Problem Management?
- PrM 2.1.1 Differences between incident management and problem management
- PrM 2.1.2 Incident vs problem

PrM 3.2 Prepare to implement Problem Management

- Good problem management relies to a great extent on a well-run incident management process. So it is sensible to implement Problem Management either in parallel with or after Incident Management.
- If resources are scarce, it is advisable to concentrate on the implementation of problem and error control (reactive problem management). When these activities reach maturity, resources can be directed to proactive problem management, which depends largely on the successful implementation of Network Monitoring and Preventative Maintenance.
- Smaller schools can introduce reactive problem management by focusing daily on the 'top 10' incidents of the previous week. This can prove to be effective, since experience shows that 20% of problems cause 80% of service degradation!

PrM 3.2.1 Risks to the implementation of Problem Management

The following can weaken the benefits of Problem Management.

- The absence of a good incident control process means that you will not have detailed historical data on incidents, which is necessary for the correct identification of problems.

- The result of lack of commitment at the top is likely to be that support staff (who are usually also involved in reactive incident control) cannot allocate enough time to structured problem-solving activities.
- In order not to undermine the service desk role, all incident reports must come through the service desk and not direct to the technician. Difficulties will arise if the service desk is dealing with multiple reports of incidents and the technician is not fully aware of the extent of the problem.
- Any failure to set aside time to build and update the call log or incident sheets will restrict the benefit of understanding the bigger picture on the network and looking at trends that may point towards an underlying problem.
- If you are unable to determine accurately the impact on the school of incidents and problems, you will not be in a position to give critical incidents and problems the correct priority.

PrM 3.2.2 Impact of implementing Problem Management

- An effective system for logging incidents is fundamental to the success of Problem Management.
- Setting achievable objectives and making use of the problem-solving talents of existing staff is a key activity. Consider 'part-time' problem management, whereby staff set aside periods when they will look at problems away from the daily fire-fighting pressures.
- In view of the potentially conflicting interests between Incident Management and Problem Management, good sense should prevail. Support staff should be aware of the importance of balancing activities between the two. For example – if the equipment is required now and a workaround is available, implement it at once, but set aside time at the end of the school day to resolve the problem.

PrM 3.2.3 Identify the users of problem management

The users of problem management will be the staff running the service desk and incident management processes. It could be said that all users of incident management are ultimately users of problem management. However, it is the decision of the service desk and technician to refer an incident to the problem management process.

PrM 3.2.4 Identify who will staff problem management

Problem management is a specialised process requiring a good grounding in technical support. It is expected that technicians will staff problem management, with input from specialists where possible. Specialist input or subscription to a support service may form part of a school's contract with a supplier.

PrM 3.2.5 Plan your problem management training

The training plan for problem management should concentrate on the service desk and technician. Users should be notified that a problem management process is to be introduced and how it will work, but they should not require any training.

- Ensure that all service desk and technical support staff understand the incident management process.
- Train the service desk staff how to progress a call from an incident to a problem.
- Train the service desk staff to identify patterns of incidents that indicate a problem.
- Train the service desk staff to record incident details in a way that will help a technician. This will be evident in feedback from the technician after the first few problems have passed through the problem management process.
- Decide on the costs involved in problem Management and produce a guide for the technician on the amount of time to allocate to resolving a problem.

PrM 3.3

The Problem Management implementation plan

Identifier	What	When	Who
1	Decide who will be your problem management technician		
2	Decide which training the technician requires		
3	Decide which training the service desk staff will require		
4	Arrange and implement the required training		
5	Decide how the service desk will pass calls to the technician		
6	Decide which documentation will be used		
7	Create or download the required incident diagnostics forms		
8	Ensure that the technician and service desk staff know how to use the forms		
9	Decide whether to use a knowledge base		
10	Decide on the format of the knowledge base		
11	Decide how to populate the knowledge base from resolved problems		
12	Ensure that the problem management process is documented		
13	Incorporate in the process any changes decided as a result of testing		
14	Decide how to record details of resolutions		
15	Decide who carries out follow-up actions and define the procedures they should follow		
16	Decide on the review process		
17	Decide how to keep staff informed		
18	Plan your first communication to the school about Problem Management		
19	Decide whether you need to run a pilot of the process		
20	Carry out the pilot and review it		
21	Incorporate changes into the system as a result of the pilot review		
22	Plan the launch date for FITS Problem Management		
23	Check that all training has occurred		
24	Launch the process of Problem Management		
25	Carry out the first review and feedback to all staff involved in the Problem Management process		

- Have a plan
- Follow the plan
- Have a fallback plan

PrM 3.3.1 Technician forms

The technician forms are designed to aid technicians in doing their job. It is always useful to record events as they occur, as this helps to ensure that you leave nothing out. If your records are not comprehensive – which may happen if you don't complete the form at the time – you may omit a seemingly obscure piece of information that later proves to be the key to resolving the incident or problem.

See Appendix A for the incident diagnostics sheet.

See Appendix B for a draft letter you may like to consider circulating at your school.

PrM 3.4 Problem Management post-implementation review

PrM 3.4.1 Problem Management reports

The aim of reports is to summarise what you already know, and in technical support to reduce the need for technical expertise to understand the information. They are also useful to summarise in non-technical language to show where improvements could be made. Often the improvements require expenditure, so having reports to back up your suggestions can prove invaluable.

- Show the average time spent on problems per week.
- Show how many problems are solved per week.
- Show the number of problems for which you consider resolution would not be cost effective.
- Once implementation is complete, compare the incident levels to the previous weeks to see if problem solving reduces incidents.
- Show the number of identified known errors and their associated workarounds produced from problem management.
- Over time, see if problem management reduces the incident management 'top 10'.
- Finally, if you implement problem management with incident management, show the number of incidents and problems each week. Over time it will become easier to identify the difference, so persevere with the reports.

Problem management reports should identify where isolating problems from incidents has provided benefit.

PrM 3.4.2 Customer satisfaction analysis and surveys

Satisfaction surveys are an excellent method of monitoring customer perception and expectation and can be used as a powerful marketing tool. However, to ensure success you should address several key points.

- Decide on the scope of the survey.
- Decide on the target audience.
- Clearly define the questions.
- Make the survey easy to complete.
- Conduct the survey regularly.
- Make sure that your customers understand the benefits.
- Publish the results.
- Follow through on survey results.
- Translate survey results into actions.

PrM 3.4.3 Measurements

- Do not set targets that cannot be measured.
- Ensure that customers are aware of what you are doing, and why.
- Establish a baseline before discussing formal service-level agreements (SLAs) with customers. See FITS Service Level Management.
- Maintain measurements of what is necessary and viable. For instance, if your staff think that they need feedback on response times – then measure them!

PrM 3.5 Problem Management resources

PrM 3.5.1 Problem-analysis tools

- Beware of overloading yourself with tools that you cannot use easily.
- Beware of thinking that you can solve all problems if you have the right tool.
- Beware of making all problems a mathematical issue and inventing models and diagrams to explain your theory!
- Remember that there is a cost associated with the time spent on problem solving, so use problem solving for expensive issues!

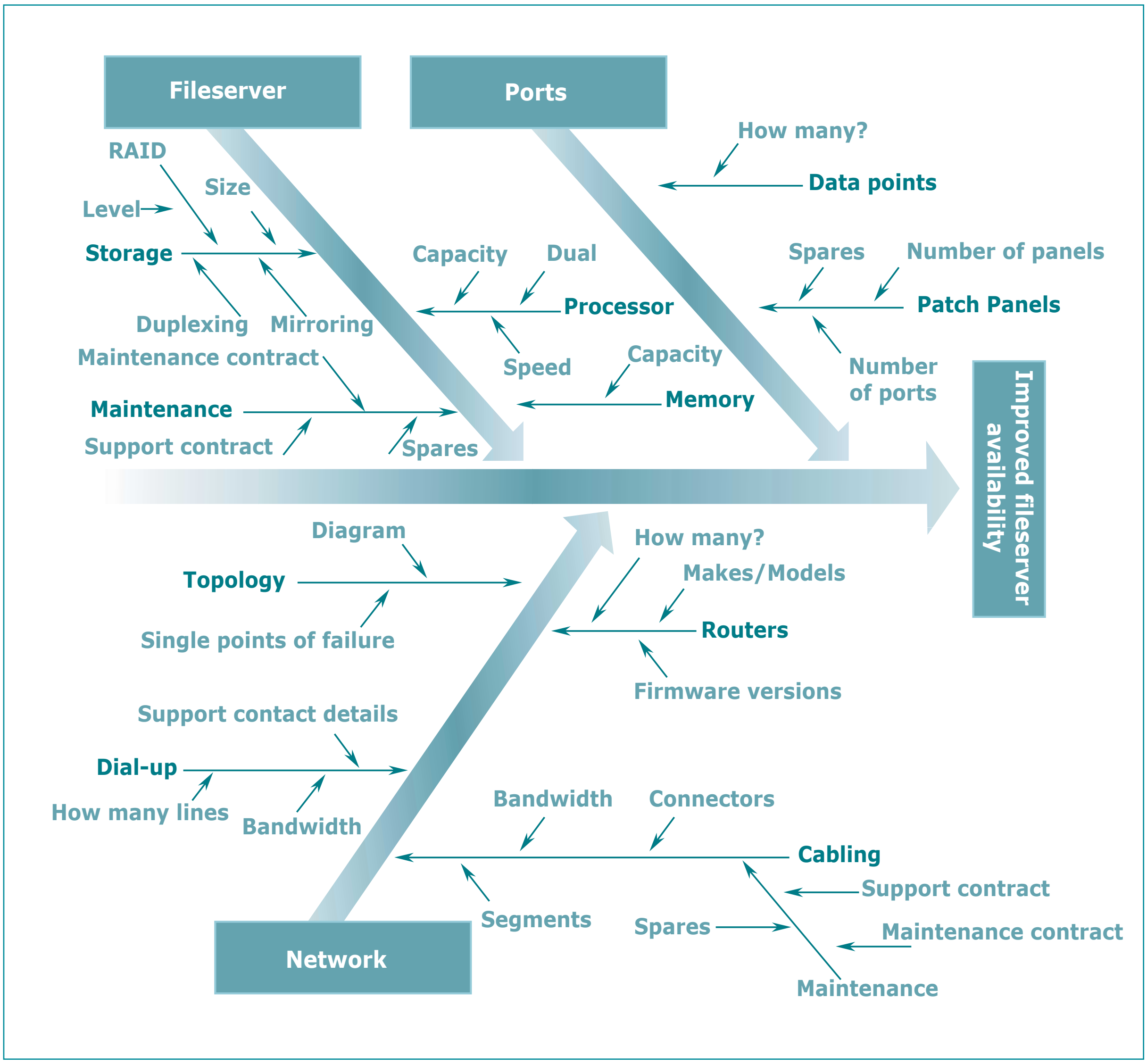
Root cause analysis

- This is the process of finding the real cause of a problem and dealing with it rather than simply continuing to deal with the symptoms.
- It seeks to identify the reason for the failure by asking lots of questions and determining whether changing an event early on in the chain of events could have prevented the failure.
- Ways to implement the change are decided and actioned through the Change Management process.

See scenario that explains root cause analysis.

Error code look-up

This is where you find out what a displayed error code means. Often the user manual or technical manual cannot be found or it does not detail the error codes of the software. Before the internet became so useful, the user or technician could not find out easily what the error meant. Using search engines you can look up the error code, the model of the equipment and the operating system to get a filtered response that may guide you towards the reason for the error.



Fishbone diagram

This diagram, also referred to as a cause-and-effect diagram or tree diagram, displays the factors that affect a particular quality, characteristic, outcome or problem. The end product is typically the result of a brainstorming session in which members of a group offer ideas on how to improve a product, process or service. The trunk of the diagram represents the main goal, and primary factors are represented as branches. Secondary factors are then added as stems, and so on. Creating the diagram stimulates discussion and often leads to increased understanding of a complex problem.

PrM 3.5.2 Technician forms

See PrM 3.3.1.

PrM 3.6 Roles and responsibilities in Problem Management

See PrM 5.

PrM 4 Operations guide

PrM 4.1 How to operate Problem Management

PrM 4.1.1 How to deal with major incidents or major problems

A major incident or problem can be classified as one which causes serious disruption to the computer service in the school. This can include:

- a virus outbreak or threat
- closure of internet services
- file server failure
- partial or total network failure
- building problems – for example, fire, smoke, flood or frost damage
- software problem affecting over 30% of computers.

PrM 4.1.1.1 Major incident process

- Service desk to field all calls and reschedule planned incident responses
- Technician to be notified of the major incident
- Technician to identify extent of problem before taking any action
- School to allocate an additional person to help the technician
- Additional person to be responsible for communication between the technician and users and to provide ad hoc help to enable the technician to deal with the incident
- Technician to discuss with the school leader the extent of the problem and a planned response (the school leader needs to know how to reschedule the planned work that involves the affected computers)
- School leader to ensure that the technician has the necessary resources to deal with the problem – including time
- Technician to decide how long to continue with trying to fix the problem before calling on the school's 'disaster recovery' option

PrM 4.1.2 The seven stages of the Problem Management process

1. Notification of a problem
2. Requesting technical support
3. Problem analysis
4. Production of theory
5. Production of resolution
6. Results of resolution
7. Problem closure

Stage 1 Notification of a problem

It is either the single point of contact at the service desk or the technician who will decide if an incident is really a problem (see overleaf). The user will notify an incident in the usual way using the incident form. When the service desk receives the form, it will be checked. With experience, service desk staff will know if this is to be passed through Problem Management. Otherwise they will pass it to the technician in the usual way.

Deciding if an incident is a problem

When service desk staff check the incident sheet, they may notice the following:

- the same type of incident reported on several other computers in the last few days
- the same type of incident reported on this computer in the last few weeks
- yet another regularly recurring fault on the same computer.

Staff can do these checks by looking at the call log or by using simple searches using a find function to spot certain words or phrases – for example 'network card', 'pc24' (if this is a computer's unique reference) or 'printer jam'.

The single point of contact (SPOC) at the service desk may record this information on the incident sheet and inform the technician when placing the call.

Stage 2 Requesting technical support

If the service desk has decided that this is a problem, it must be passed to the technician and no further diagnostic work is required by the service desk.

The technician is informed in the usual way about the call and the person on the service desk will advise why they think it should be treated as a problem.

If the school has 'swap-out spares' that a competent person in the school can install, the technician may advise doing this before any further work is done to the faulty equipment. The benefits would be:

- time saved waiting for the technician to attend to the call
- reduction in time the equipment is unavailable
- an opportunity for the technician to investigate the problem without being under time pressure.

Stage 3 Problem analysis

Problem analysis uses common sense, asks lots of questions and should not be too far fetched with the final theory.

Technicians should remember that using phrases like 'power line glitch', 'infrequent reset phenomenon', 'intermittent random fluctuating memory address' and other such odd-sounding phrases do not impress the user. If you are not sure what is happening then say so. Honesty is the best policy. As long as you have an answer – which may be to replace the equipment or that a purchase is required – this is fine.

See PrM 3.5.1 for problem analysis tools.

Stage 4 Produce theory

From the evidence, analysis and experience, produce a theory for what is happening – or what has happened.

Then use the theory of 'what went wrong' to produce action to resolve the problem. Your first theory may not always be correct and you should try to show why this is. Avoid theories you can't explain!

Stage 5 Produce resolution

Pause before taking action.

Write down exactly what was done and the outcome. Do this for every action you took – even if it consisted of just one line of a system set-up file.

The step-by-step actions should be able to be traced to find out what the technician did to resolve the problem and therefore help in resolving future problems. Problem management is a huge learning curve, so making notes, although time consuming, is very important.

Stage 6 Results of resolution

The results of the resolution may affect many systems in the school. If a plan is to be drawn up to replicate the actions across other systems, this must be done using the process described in Change Management.

Stage 7 Problem closure

Update the incident diagnostics sheet and the incident sheet and pass them to the service desk.

The service desk performs the usual call closure operations.

PrM 4.2 When does Problem Management occur?

Problem Management is a reactive and a proactive process.

The reactive aspect of Problem Management does not require immediate response. It is worth while setting aside time during the week to devote to problem management: it requires careful thought and cannot be hurried. The technician will need to be left undisturbed to work on it and should not be required to be in attendance for incidents. This approach should ensure an effective result from the process, which will benefit the school.

The proactive aspect is to monitor equipment and analyse incidents. The results of monitoring should be analysed to detect potential problems and provide a solution that can be implemented before failure. An example of this is to monitor disk space usage to remove temporary files, to archive files and to clean up disks before they become full and create network-wide problems.

Checking logged incidents can show trends such as printing problems where, for example, one printer often fails to complete printing and will print text but not pictures. It could be that this call is only logged occasionally, but if it was found and the user told that this printer can't do this type of print it would save the time of the user and technical support as there is no fault to report. Problem analysis may indicate that a small memory upgrade to the printer is all that is required or that it would print the picture if it were a different file type. Ultimately getting the best use out of the printer may avoid the expense of replacing the printer.

PrM 4.3 Who carries out Problem Management?

Problem Management usually starts with an incident or as a result of monitoring.

- The service desk will investigate an incident and after following guidelines will decide whether it is a problem for deeper investigation and analysis.
- A technician will start working on an incident and decide if it is a problem.
- Network monitoring will highlight areas that need further checking to find out whether there is a potential problem.

See also PrM 5.

Problem management is the 'black art' bit of technical support. From the evidence, analysis and experience technicians produce a theory for what is happening or has happened. The theory needs to be believable, so before taking action you should show why your theory might work. You produce an approach to resolving the problem, check it for soundness and then implement it. This is an iterative process that you may have to go through several times before you find the correct solution.

PrM 4.4 Problem Management resources

See PrM 3.5.

PrM 4.4.1 Technician forms

See PrM 3.3.1.

PrM 4.4.2 Problem Management checklist

- Do you spot problems before an incident occurs?
- Do you record resolutions for future reference?
- Do you resolve known errors before they become an incident?
- Do you minimise the adverse effect on users when an incident occurs?
- Do you analyse incident trends to prevent further incidents?
- Do you allocate enough time for problem management and do you review the allocation periodically?

PrM 4.5 Problem Management reports

See PrM 3.4.1.

PrM 5 Roles and responsibilities

- Service desk to note on the incident sheet that the problem has been passed to problem management
- Service desk to log, monitor and track the progress of the problem
- Service desk or technician to spot trends
- Technician support to action problems raised from incident management
- Technician support to progress unresolved incidents through the problem management process
- Technician assisting with the handling of major incidents and identifying the root causes
- Technician preventing the replication of problems across multiple systems
- Any additional first-line support groups, such as configuration management or change management specialists to be consulted
- Second-line and third-line support groups, including specialist support groups and external suppliers
- User to keep the service desk informed of any further changes to the state of the affected equipment (sometimes computers start working again when different incidents are resolved)

Additional functions that form part of Problem Management

- Developing and maintaining the problem control process
- Reviewing the efficiency and effectiveness of the problem control process
- Producing management information
- Allocating resources for the support effort
- Monitoring the effectiveness of error control and making recommendations for improving it
- Developing and maintaining problem and error control systems
- Reviewing the efficiency and effectiveness of proactive Problem Management activities

The scale depends on the time required for the Problem Management process.

See also PrM 2.2.

PrM 6 Review of Problem Management

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

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

PrM 6.1 Recap of Problem Management

The overview describes problem management and explains the differences between incidents and problems. Problem management can be time consuming and we give advice about when to use the process. An implementation guide provides step-by-step instructions on planning and introducing problem management. The operations guide shows the stages of problem management, with the diagnostic work that a technician needs to do. It stresses the importance of keeping records to enable the sharing of results. For quick reference we also set out in separate areas the roles and responsibilities involved and the resources you will need.

Check your understanding of the process by going through sections PrM 6.1.1 to PrM 6.1.4 below.

PrM 6.1.1 Problem Management summary

Step	Tasks
Prepare to implement.	• Identify the users of problem management. • Identify who will staff the Problem Management process. • Plan your training. • Consider the impact of problem management. • Assess the risks of using problem
Define what needs to be done.	• Ensure that you are recording your calls and can track progress. • Understand the difference between problems and incidents. • Have a process to separate incidents from problems. • Decide how much time each week to devote to problem management. • Choose which areas to improve and which processes to remove. • You need to sell the idea to other staff, so make sure you're happy with it first

Step	Tasks
Implement problem management.	• Follow the implementation plan. • Train technicians in diagnostic techniques. • Write a letter to all users about the introduction of the new service.
Problem management resources	• Incident management resources such as incident diagnostics sheet • Fishbone diagrams • Root cause analysis • Instructions on the use of the forms • Known error database • Workaround techniques
Post-implementation review	• Workload monitoring • Analysis, surveys and measurements • Problem reports

PrM 6.1.2

What you should expect now that you have implemented Problem Management

- You have a process for dealing with major incidents.
- Everyone understands that problems usually start as incidents which are escalated into problems once diagnosed by the technicians.
- Technicians understand how and when to reserve time to deal with problems.
- Everyone understands that problem management is a proactive process, and that the related reactive process is incident management.
- You appreciate that problem management takes time, can be expensive and should only be used for recurring or expensive incidents.
- You understand the costs involved in problem management.

PrM 6.1.3

What you should have achieved through Problem Management

- You now have a formal process for dealing with problems.
- You have a method for introducing workarounds.
- You have set up a major incident process.
- You have a systematic method for deciding when an incident becomes a problem.
- You have information about the amount of technician time required to resolve problems.
- You have developed a consistent approach to recording actions taken as part of problem management and the results of the resolutions applied.
- You have at your fingertips information about the number of problems currently outstanding and how long they have been logged.
- You now have a process for checking whether problem management reduces the 'top 10' incident list.

PrM 6.1.4 Benefits of having implemented Problem Management

- A proactive approach reduces the disruption to service when errors occur.
- The school has faith in the quality of the technical support, with reducing costs and high motivation for both users and technicians.
- You save time by using a standard approach to every problem.
- There is a reduction in the number of recurring incidents.
- Permanent solutions mean a gradual reduction in the number and impact of problems and known errors, as those that are resolved stay resolved.
- The process provides the historical data to identify trends, and the means of minimising failures and of reducing the impact of failures.
- You achieve a better first-time fix rate of incidents as a result of having a knowledge database available to the service desk and technicians when a call is first logged.
- You can co-ordinate your management information to enable better service.
- You have a way of checking that suppliers and staff are meeting agreed service levels.

PrM 6.2 Checklist

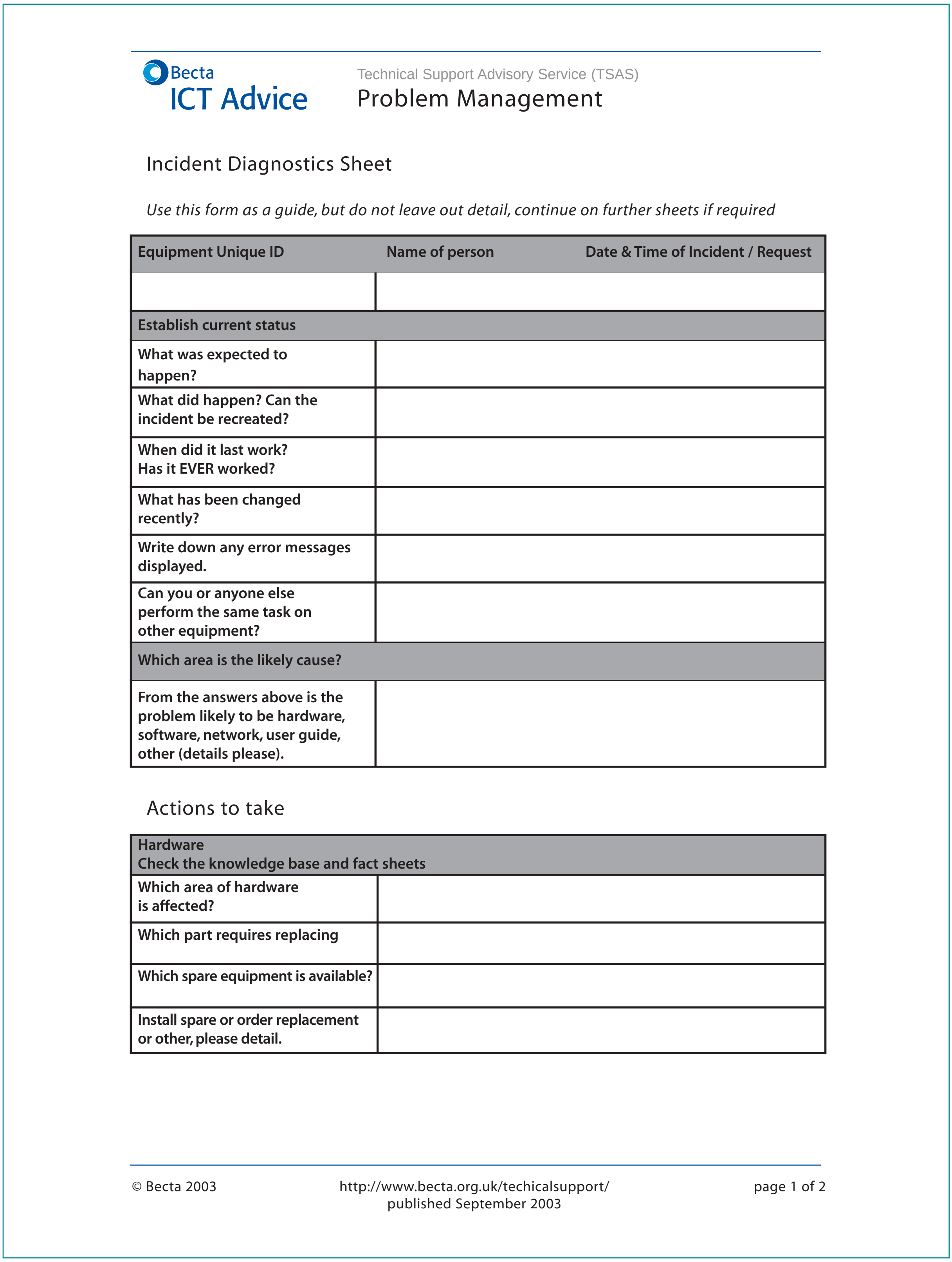
Use this checklist to identify any areas of problem management that have not been entirely successful. Then reinforce them by revisiting and re-implementing the relevant section of the FITS process.

Characteristics of a successful implementation	FITS section to revisit if implementation has not yet been successful	
Everyone understands the process for deciding when an incident becomes a problem.	PrM 4.1.2	Stage 1 of the Problem Management process – Deciding if an incident is a problem
Staff understand and apply the process for dealing with major incidents.	PrM 4.1.1	How to deal with major incidents or major problems
There is an overall understanding that problem management is a proactive process.	PrM 4.2	When does Problem Management occur?
The production of reports about problems is helping to reduce the workload of the technical support team.	PrM 3.4.1 PrM 5	Problem Management reports Roles and responsibilities
Technicians and the service desk staff understand the stages of problem management.	PrM 4.1	How to operate Problem Management
The technicians can use problem-analysis tools.	PrM 3.5.1	Problem-analysis tools

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

Appendices

PrM Appendix A Incident diagnostics sheet



Becta
ICT Advice

Technical Support Advisory Service (TSAS)

Problem Management

Incident Diagnostics Sheet

Use this form as a guide, but do not leave out detail, continue on further sheets if required

Equipment Unique ID	Name of person	Date & Time of Incident / Request
Establish current status		
What was expected to happen?		
What did happen? Can the incident be recreated?		
When did it last work? Has it EVER worked?		
What has been changed recently?		
Write down any error messages displayed.		
Can you or anyone else perform the same task on other equipment?		
Which area is the likely cause?		
From the answers above is the problem likely to be hardware, software, network, user guide, other (details please).		

Actions to take

Hardware Check the knowledge base and fact sheets	
Which area of hardware is affected?	
Which part requires replacing	
Which spare equipment is available?	
Install spare or order replacement or other, please detail.	

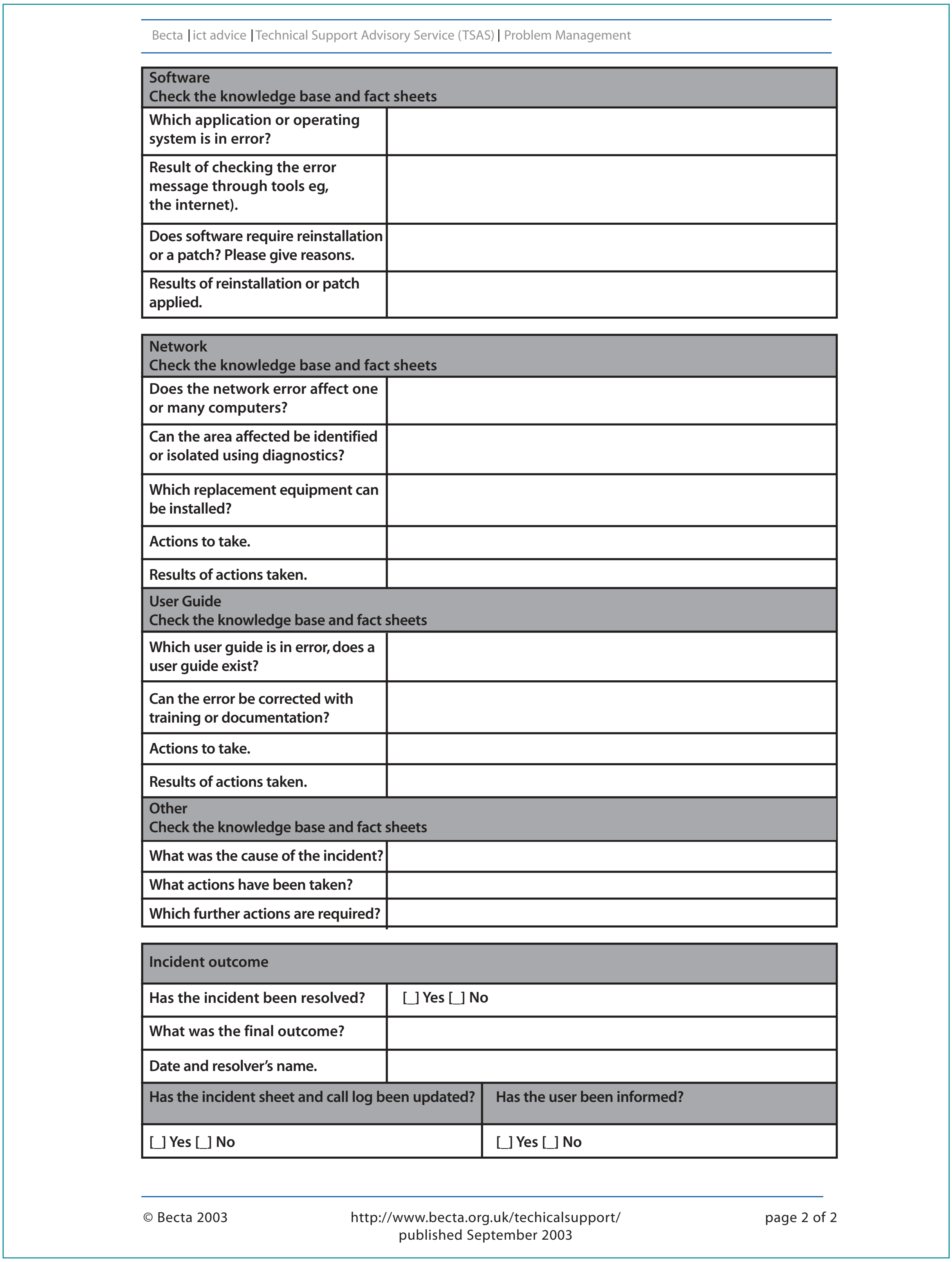
© Becta 2003

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

page 1 of 2

You can download a template from the FITS website [**http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=problem&id=dw1098_1**].

PrM Appendix A Incident diagnostics sheet



Becta | ict advice | Technical Support Advisory Service (TSAS) | Problem Management

Software Check the knowledge base and fact sheets	
Which application or operating system is in error?	
Result of checking the error message through tools eg, the internet).	
Does software require reinstallation or a patch? Please give reasons.	
Results of reinstallation or patch applied.	

Network Check the knowledge base and fact sheets	
Does the network error affect one or many computers?	
Can the area affected be identified or isolated using diagnostics?	
Which replacement equipment can be installed?	
Actions to take.	
Results of actions taken.	
User Guide Check the knowledge base and fact sheets	
Which user guide is in error, does a user guide exist?	
Can the error be corrected with training or documentation?	
Actions to take.	
Results of actions taken.	
Other Check the knowledge base and fact sheets	
What was the cause of the incident?	
What actions have been taken?	
Which further actions are required?	

Incident outcome	
Has the incident been resolved?	[_] Yes [_] No
What was the final outcome?	
Date and resolver's name.	
Has the incident sheet and call log been updated?	Has the user been informed?
[_] Yes [_] No	[_] Yes [_] No

© Becta 2003 http://www.becta.org.uk/techicalsupport/ page 2 of 2
published September 2003

You can download a template from the FITS website [**http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=problem&id=dw1098_1**].

PrM Appendix B Document to users about the introduction of Problem Management

Dear _______,

Introduction of Problem Management to our school

We have decided to introduce Problem Management as a complementary service to Incident Management. This will enable the technical support function to pinpoint recurring incidents and common errors and focus on solving them for good.

This service should enhance the approach the technicians use for finding out why problems occur and will enable us to keep the computer systems working as efficiently as possible for you. Training in this process will be provided for the service desk single point of contact and the technicians. Everyone else should continue to log their calls in the usual way, so please remember to use the incident sheet to log all calls with the service desk.

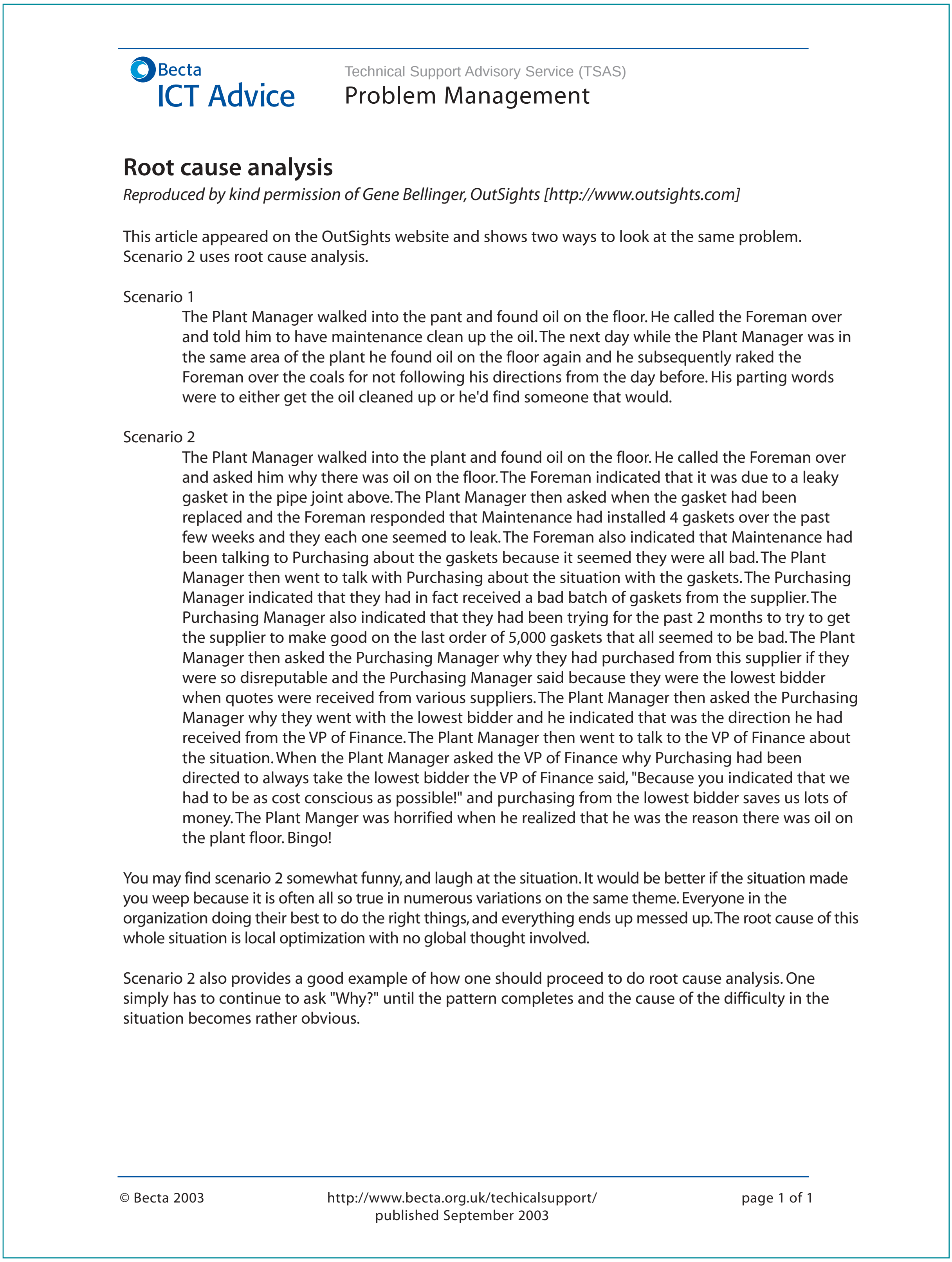
You should benefit from:

- a reduction in the number of repeat incidents
- faults found before they affect you, with resolutions implemented out of working hours, so that you don't experience any downtime
- efficient handling of any major incident (such as a virus outbreak) that may occur.

The new service is scheduled to start on xxxxxx, and we shall publish more details nearer the start date.

You can download a template from the FITS website [**http://www.becta.org.uk/tsas/index.cfm?refsect=ntss&bcsect=default&sect=problem&id=dw1175**].

PrM Appendix C Root cause scenario – example



Becta
ICT Advice

Technical Support Advisory Service (TSAS)
Problem Management

Root cause analysis

Reproduced by kind permission of Gene Bellinger, OutSights [http://www.outsights.com]

This article appeared on the OutSights website and shows two ways to look at the same problem. Scenario 2 uses root cause analysis.

Scenario 1

> The Plant Manager walked into the pant and found oil on the floor. He called the Foreman over and told him to have maintenance clean up the oil. The next day while the Plant Manager was in the same area of the plant he found oil on the floor again and he subsequently raked the Foreman over the coals for not following his directions from the day before. His parting words were to either get the oil cleaned up or he'd find someone that would.

Scenario 2

> The Plant Manager walked into the plant and found oil on the floor. He called the Foreman over and asked him why there was oil on the floor. The Foreman indicated that it was due to a leaky gasket in the pipe joint above. The Plant Manager then asked when the gasket had been replaced and the Foreman responded that Maintenance had installed 4 gaskets over the past few weeks and they each one seemed to leak. The Foreman also indicated that Maintenance had been talking to Purchasing about the gaskets because it seemed they were all bad. The Plant Manager then went to talk with Purchasing about the situation with the gaskets. The Purchasing Manager indicated that they had in fact received a bad batch of gaskets from the supplier. The Purchasing Manager also indicated that they had been trying for the past 2 months to try to get the supplier to make good on the last order of 5,000 gaskets that all seemed to be bad. The Plant Manager then asked the Purchasing Manager why they had purchased from this supplier if they were so disreputable and the Purchasing Manager said because they were the lowest bidder when quotes were received from various suppliers. The Plant Manager then asked the Purchasing Manager why they went with the lowest bidder and he indicated that was the direction he had received from the VP of Finance. The Plant Manager then went to talk to the VP of Finance about the situation. When the Plant Manager asked the VP of Finance why Purchasing had been directed to always take the lowest bidder the VP of Finance said, "Because you indicated that we had to be as cost conscious as possible!" and purchasing from the lowest bidder saves us lots of money. The Plant Manger was horrified when he realized that he was the reason there was oil on the plant floor. Bingo!

You may find scenario 2 somewhat funny, and laugh at the situation. It would be better if the situation made you weep because it is often all so true in numerous variations on the same theme. Everyone in the organization doing their best to do the right things, and everything ends up messed up. The root cause of this whole situation is local optimization with no global thought involved.

Scenario 2 also provides a good example of how one should proceed to do root cause analysis. One simply has to continue to ask "Why?" until the pattern completes and the cause of the difficulty in the situation becomes rather obvious.

© Becta 2003 http://www.becta.org.uk/techicalsupport/ page 1 of 1
published September 2003

Glossary

10Base-T

A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 10Base-T is based on the older Ethernet standard but is 10 times faster than Ethernet; it is often referred to as Fast Ethernet. Officially, the 10Base-T standard is IEEE 802.3u. Like Ethernet, 10Base-T is based on the CSMA/CD LAN access method.

AppleTalk

Inexpensive LAN (local area network) architecture built into all Apple Macintosh computers and laser printers. AppleTalk supports Apple's LocalTalk cabling scheme, as well as Ethernet and IBM Token Ring. It can connect Macintosh computers and printers, and even PCs if they are equipped with special AppleTalk hardware and software.

Asset

Component of a business process. Assets can include people, accommodation, computer systems, networks, paper records, fax machines, etc.

Availability

Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio: the proportion of time that the service is actually available for use by customers within the agreed service hours.

Availability Management

To ensure that ICT services are available for use consistently as agreed.

Bandwidth

The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps).

Baseline

A snapshot or a position which is recorded. Although the position may be updated later, the baseline remains unchanged and available as a reference of the original state and as a comparison against the current position.

Bridge

A device that connects two LANs (local area networks), or two segments of the same LAN that use the same protocol, such as Ethernet or Token Ring.

Buffer

A temporary storage area, usually in RAM. The purpose of most buffers is to act as a holding area, enabling the CPU to manipulate data before transferring it to a device.

Build

The final stage in producing a usable configuration. The process involves taking one or more input configuration items and processing (building) them to create one or more output configuration items (eg software compile and load).

Capacity

Ability of available supply of processing power to match the demands made on it by the business, both now and in the future.

Capacity Management

To ensure that all ICT processing and storage capacity provision match present and evolving needs.

Category

Classification of a group of configuration items, change documents, incidents or problems.

Change

The addition, modification or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.

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

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

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

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

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