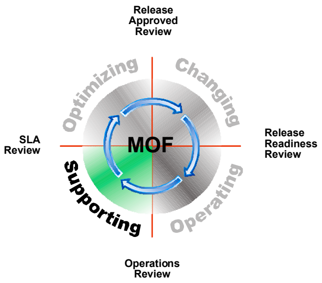
Microsoft®

MOF Service Management Function Problem Management

patterns & practices



Microsoft®

Solutions for Management

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Contents

Document Purpose

This guide provides detailed information about the problem management service management function (SMF) for organizations that have deployed, or are considering deploying, Microsoft technologies in a data center or other type of enterprise computing environment. This is one of the more than 20 SMFs defined and described in Microsoft® Operations Framework (MOF). The guide assumes that the reader is familiar with the intent, background, and fundamental concepts of MOF as well as the Microsoft technologies discussed.

An overview of MOF and its companion, Microsoft Solutions Framework (MSF), is available in the *Introduction to Service Management Functions* guide. This overview guide also provides abstracts of each of the service management functions defined within MOF. Detailed information about the concepts and principles of each of the frameworks is also available in technical papers available at www.microsoft.com/solutions/msm/.

Executive Summary

All businesses that rely on information technology (IT) will experience incidents that cause some level of disruption to their operation. Many organizations become expert at dealing with these types of service interruptions and go on to develop extremely competent incident management processes and procedures. Support staff can often be very proud of the speed and the skills they have been able to deploy in restoring services.

Unfortunately, this focus can lead to support organizations concentrating on recovering from incidents, rather than resolving the underlying root causes. This results in recurring incidents that reduce both customer satisfaction and the cost-effectiveness of the support process. By implementing problem management processes at the same time as incident management processes, organizations can identify and resolve the root causes of any significant or recurring incidents, thus reducing the likelihood of recurrence.

In order to achieve this, problem management investigates and analyzes the root causes of incidents and commonly initiates changes to internal processes, procedures, or the infrastructure to resolve the underlying problem or provide a temporary workaround.

Key benefits of effective problem management include:

- A reduction in the number and business impact of incidents, problems, and known errors as problem management begins to resolve the root causes of incidents and deploy effective workarounds.

- Improved IT service quality as customers experience fewer repeat incidents.
- Increased cost effectiveness of support resources will occur as steps are taken to reduce the time spent by support teams in repetitive, time consuming, and costly support tasks. Resources can then be focused more efficiently on identifying the causes of incidents.
- Increased knowledge capital (the historic data used to identify trends and proactively identify any problem areas). This should reveal information about individual components within the infrastructure, as well as process or procedural breakdowns, and provide data for future problem analysis.
- Improved organizational learning can take place as accurate recording of problem management data leads to trending and identification of areas that really require attention.
- Increased first-time fix rate at the service desk as workarounds can be deployed to increase the speed of service restoration.
- Timely identification, diagnosis, and resolution of problems.
- Complete resolution of problems as underlying causes are identified and corrected.

Process and Activities

Problem Management Overview

The problem management SMF aims to ensure that all problems and known errors affecting the IT infrastructure are identified and recorded. Recording problems and known errors ensures that all problems can be managed and tracked during their life cycle, providing valuable information for other SMFs, such as incident management, change management, and service desk. The process ensures that any underlying problems identified are associated with the corresponding incidents that have occurred. Additionally, the process works to identify suitable workarounds that provide customers with service restoration or service improvement while a more permanent solution is sought.

Problems undergo classification, which is done by assessing the business impact and analyzing the urgency and the resources required to effect temporary or permanent solutions to the problems. This classification ensures that problems are correctly prioritized and routed to an appropriate resolution group.

Problems impacting the business can occur in a number of areas. When investigating possible workarounds or solutions to identified problems, problem management may make requests for changes to the IT infrastructure, internal procedures, user training, or any other elements affecting service.

The problem management process should also deploy technologies to proactively prevent problems from occurring, such as working with availability management to ensure that increased redundancy is built in to critical infrastructure areas.

Problem management performs investigation and diagnosis in a similar fashion to the incident management process. However, the focus is entirely different. Incident management is concerned with deploying procedures and activities to rapidly restore service, while problem management identifies the root cause of incidents impacting the business. The problem management process provides the structure to ensure that all problems are owned, tracked, and monitored throughout the problem life cycle.

This document illustrates the processes and activities involved in problem management, coupled with the ways in which problem management relates to other SMFs in the MOF process model.

Goals and Objectives

The goal of problem management is to minimize the adverse impact on the operational ability of a business due to incidents and problems caused by errors within the IT infrastructure and to prevent the recurrence of incidents related to these errors. In order to achieve this goal, problem management seeks to establish the root cause of incidents and then initiate actions to improve or correct the situation.

The objectives of problem management are to:

- Identify and take ownership of problems affecting infrastructure and service.
- Take steps to reduce the impact of incidents and problems.
- Identify the root cause of problems and initiate activity aimed at establishing workarounds or permanent solutions to these identified problems.
- Using recorded problem and incident data, perform trend analysis to predict future problems and enable prioritization of problem management activity.

The problem management process has both reactive and proactive aspects. The reactive elements provide direct support to the day-to-day operational activities of other service management functions, such as incident management, and are concerned with initiating activity aimed at resolving problems in response to one or more incidents currently causing issues.

Proactive problem management is concerned with identifying problems and known errors before incidents occur.

Scope

Problem management is concerned with the identification and recording of problems impacting IT service. Frequently incidents occur as the result of underlying root causes, and it is these that problem management seeks to identify and record as problems. The function then determines how the problem can be resolved, and what the priority for resolution is. It seeks to determine temporary workarounds that can be used by the service desk and incident management SMFs to quickly restore service. It is also responsible for the successful correction of any known errors that have been identified.

Problem management seeks to change IT infrastructure components to remove known errors and thus prevent any recurrence of incidents. Problem management also addresses procedures or practices that may be the cause of problems. Problem management is concerned with both the live and development environments and directly interfaces with, and operates alongside, change management processes.

Proactive problem management is concerned with identifying underlying problems to prevent incidents before they occur.

Conducting trend analysis of problem management data and incident records helps to achieve this. The function is also concerned with reviewing the causes and handling of major incidents and major problems. Monitoring and tracking of all problems takes place during the entire problem/error life cycle.

Problem management relies on effective, accurate, and consistent incident management to be able to function efficiently. However, problem management has an entirely different focus. Incident management aims to restore service as soon as possible, whereas problem management seeks to identify the root cause of the incident or incidents.

Key Definitions

Impact. A measure of how the problem or incident affects a customer or the business.

Incident. Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of service.

Known error. A problem that has been successfully diagnosed and for which a permanent alternative or temporary circumvention exists. If a business case exists, an RFC will be raised, but, in any event, it remains a known error unless it is permanently fixed by a change.

Major incident. An incident with a high impact or potentially high impact, which requires an immediate response that is above and beyond that given to "normal" incidents. Typically these incidents require cross-company coordination, management escalation, the mobilization of additional resources, and increased communications.

Major problem. A problem with a high impact or potentially high impact, which requires a response that is above and beyond that given to "normal" problems. There are normally longer timescales available in which to plan a resolution to a major problem compared to a major incident, which often requires an immediate response. This means that it is better to treat the issue as a proactive requirement and manage it as a problem management issue. If the problem is left to incident management, because it lacks the immediacy of other incidents, there is a risk of it not being progressed. An example of a past major problem is the year 2000 issue. Typically these problems require cross-company coordination, management escalation, the mobilization of additional resources, and increased communications inwardly and outwardly.

Priority. The resulting analysis of impact and urgency.

Problem. The unknown cause of one or more incidents.

Resolution. The action taken to resolve the underlying cause.

Root cause analysis. Activity undertaken aimed at establishing the root cause of problems.

Service desk. A function that provides the vital day-to-day contact point between customers, users, IT services, and third-party organizations. The service desk not only coordinates the incident management process, but also provides an interface for many other service requests.

Solution/permanent fix. An identified means of resolving an incident or problem that provides a resolution for the underlying cause.

Trend analysis. A study of historical incident, problem, and known error data aimed at identifying future activity to reduce or prevent incidents.

Urgency. The timescale within which the incident or problem should be resolved.

Workaround. An identified means of resolving a particular incident, which allows normal service to be resumed but does not actually resolve the issue that caused the incident in the first place.

Major Processes

Problem management can be graphically presented in the form of a process flow diagram that identifies the activities that need to take place in order to ensure that the adverse impact from incidents and problems is minimized and that recurrence of the incidents is prevented.

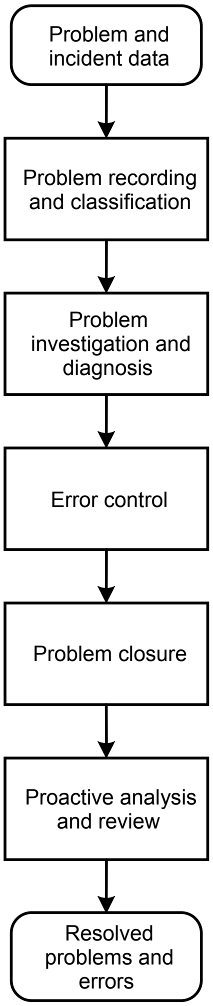

Problem and incident data
Problem recording and classification
Problem investigation and diagnosis
Error control
Problem closure
Proactive analysis and review
Resolved problems and errors

Figure 1

Problem management process flow chart

Problem Recording and Classification

This process deals with the initial detection and recording of a problem, which can originate from a variety of sources and mediums. Problems may be reported through the incident management process or as a result of analysis from the data collected by the problem management team. Additionally, other SMFs such as availability management and capacity management might detect problems and pass this information to the problem management team. It is important that problems be linked to existing incidents and that all problems are recorded in order to facilitate prioritization of problem resolutions. Once a problem has been recorded, it is assessed against the business impact of the problem and the urgency of the required resolution. This assessment determines the problem classification.

Problem Investigation and Diagnosis

This process deals with the investigation of the problem and the diagnosis of the root cause. This data can then be used to help the problem management team assess the resources and skills required to resolve the cause of the problem. The process includes dealing with major problems that require additional planning, coordination, resources, and communication, and which may result in a formal project being initiated.

Error Control

Error control covers the processes involved in successful correction of known errors. The objective is to change IT components or procedures to remove known errors affecting the IT infrastructure and thus prevent any recurrence of incidents. Many IT departments are concerned with error control, and it should be recognized that error control spans both the live and development environments. It directly interfaces with and operates alongside the change management process. Error control is the element within problem management that is responsible for seeing the problem through to a final resolution.

Problem Closure

Problem resolution details need to be fully recorded in the problem management system. It is vital to save data on the configuration items (CIs), symptoms, and resolution or circumvention actions relating to all problems so as to build up the organization's knowledge capital. This data is then available for incident matching, providing guidance during further investigations on resolving and circumventing incidents, and for providing management information. Following successful implementation of changes to resolve errors, the relevant known error record can be closed, together with any associated incident or problem records. During the problem closure process, consideration should be given to inserting an interim status statement—"Closed pending PIR"—on the incident, known error, and problem records in order to ensure that the fixes have actually worked. A post-implementation review (PIR) can then confirm the effectiveness of the solution prior to final closure.

For incidents, this might involve nothing more than a telephone call to the user to ensure that they are no longer experiencing the problem. For more serious problems and known errors, a formal review may be required.

Proactive Analysis and Problem Reviews

Proactive Analysis

Proactive analysis activities are concerned with identifying and resolving problems and known errors before incidents occur, thus minimizing the adverse impact on the service and business as a whole. The main activities are trend analysis and the targeting of preventive action.

Problem prevention ranges from prevention of individual problems, such as repeated difficulties with a particular feature of a system, to strategic decisions to fundamentally change some elements or the entire infrastructure. The latter may require major expenditure to implement, similar to the investment many organizations made in the build-up to the year 2000.

Problem Reviews

Following a major incident or a major problem, a review of all the events and actions that took place should be conducted. This review provides a means of gathering useful data for future analysis and ensures that all important lessons are identified and recorded.

The appropriate people involved in the resolution of the incident or problem should be called in to take part in the review to help determine the following:

- What was done correctly.
- What was done incorrectly.
- What could be done better the next time.
- How to prevent recurrence.
- How to quickly spot if a recurrence is happening.

Problem Recording and Classification

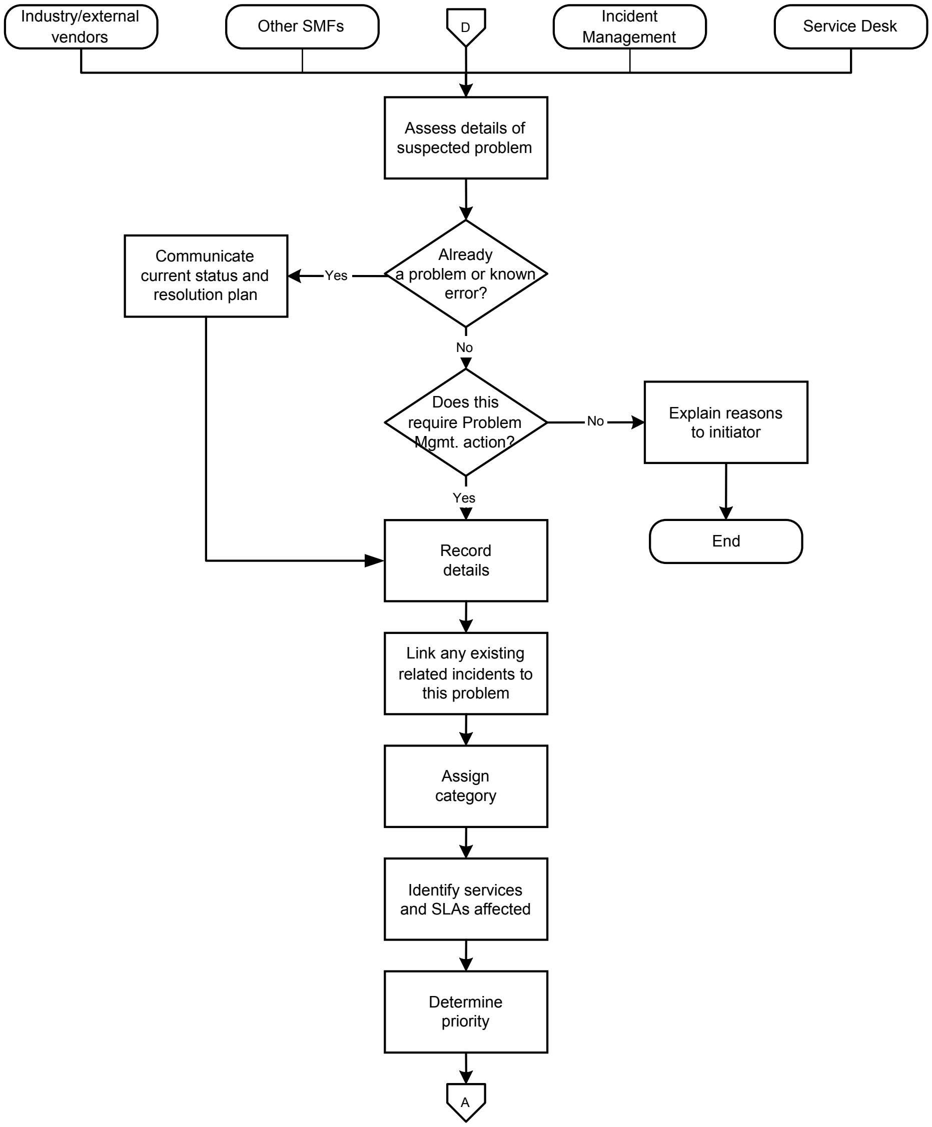

Industry/external vendors
Other SMFs
D
Incident Management
Service Desk
Assess details of suspected problem
Already a problem or known error?
Yes
Communicate current status and resolution plan
No
Does this require Problem Mgmt. action?
No
Explain reasons to initiator
End
Yes
Record details
Link any existing related incidents to this problem
Assign category
Identify services and SLAs affected
Determine priority
A

Figure 2

Problem recording process flow chart

Sources of Problem Information

The problem management team should gather information from a variety of sources that can be used to assist in the analysis of incidents and problems. The following factors are often valuable sources of this data.

External vendors. Manufacturers can provide the problem management team with valuable information about components and infrastructure items that they are producing. They commonly produce information on known errors that either they or other organizations using the products have experienced. Suppliers can provide information about upgraded products that can be used to resolve known errors.

Users of the service. Users of the service can provide additional information about how the service is affected or important background information concerning the operational requirements of the services that are affected.

Forums and user groups. User groups can be an excellent source of information for solutions to problems and can save valuable and costly investigation and diagnostic time.

Log files. Event logging facilities are commonly provided by software suppliers to aid the capture of critical data at the point of a failure. These event logs can then later be analyzed to provide support analysts with a history of events and activity taking place at the point of failure.

Incident and problem records. Incident records contain information about services that have experienced difficulty. This is especially useful if the information is recorded accurately and consistently. Problem management records contain information about current and past problems that have been identified. Again, for this information to be useful, it is essential that it be recorded accurately and consistently.

Other SMFs. Other service management functions, such as service desk, capacity management, or availability management, can provide valuable information to the problem management team for analysis.

Development cycle. Development teams know of known errors identified during other development projects, and this information should be made available to the problem management function for inclusion in the known error database.

Internet. The Internet is a valuable repository of information and contains many useful sites, user communities, supplier information pages, FAQs, and a host of other sources of information, which can be used by a problem management team for analysis.

Assessing Suspected Problems

Once a potential problem has been flagged, it needs to be assessed to see if the issue has already been recorded as a problem or a known error record. If a record exists, there needs to be an increase in the "incident count." The incident count is a record of the number of times that this particular problem or known error has resulted in an incident. The size of the incident count assists with prioritization by giving an indication of the frequency of occurrence and thus the impact this issue is having on the business.

If there is no previously established data recorded for this potential problem, then problem management needs to confirm that it meets the criteria for being considered a problem. If problem management determines that the issue is not considered a problem at the current time, perhaps because it is thought to be a one-time occurrence with a minimal impact, then they need to inform the originator of their reasons.

A problem is identified as a problem when one of the following takes place:

- The symptoms of a single significant incident do not match those of existing problems or known errors. A significant incident is one that has impacted or potentially could impact agreed service levels.
- Analysis of incident data reveals the same (repeat) incidents are commonly taking place.
- Analysis identifies multiple incidents with matching symptoms, which do not correspond to an existing problem or known error.
- Analysis of the IT infrastructure identifies a problem that could potentially lead to incidents in the future.
- Another SMF or an external source highlights an issue to problem management that could potentially lead to incidents in the future.

Some problems may be identified by personnel outside the problem management team, for example, by technical architects involved in the capacity management or availability management functions. Much of the availability management process is concerned with the detection and avoidance of incidents and problems affecting the availability of services. A synergy between availability management and problem management is thus an invaluable aid to improving service quality. Regardless of this, all problems should be notified and recorded using the problem management process.

Once a problem has been identified or detected, it must be accurately recorded. Problem records are very similar to incident records and need to be recorded in a suitable database, ideally integrated with the configuration management database (CMDB). A problem record should contain all relevant and current information about the problem. It should also be linked to any incidents or change requests that have been associated with the problem. Additionally, any permanent solutions or workarounds associated with the problem should be recorded in the relevant problem records for others to access should related incidents occur.

Problem Recording

The problem management team is responsible for retaining ownership of problems. However, individual problems requiring specialist skills should be assigned to appropriate resolver groups or, if necessary, a specially assembled team with the skills required to resolve a more complex issue. The problem should remain under the control of the problem management team throughout its life cycle. Any activity that takes place connected with the problem should be recorded in the problem record for future reference by all support staff members involved in activities connected with the problem.

Problem Record Contents

Problem records need to contain a number of specific fields for recording essential information required by the problem management process. The following items should be typical of fields contained in a problem record:

Contact information/originator. There needs to be a record of who reported the problem as he or she may be required to provide further information to specialist support personnel involved in the investigation and diagnosis. When the problem has been identified proactively by problem management, resolver groups, or another SMF, this field may identify a specific customer or person responsible for the service.

A unique problem number. Each problem will have a unique identifying number or code used for reference purposes.

Incident count/linking incidents. The problem needs to be linked to any corresponding incidents that have occurred. References to any incidents with matching symptoms should be included in the problem record. This allows the impact of the problem to be properly assessed, allows support staff to find identified workarounds, and enables incident owners to be informed when a workaround or resolution is identified.

When an incident is linked to a problem, then each time the same incident occurs, the incident count recorded in the problem record will be incremented. This gives valuable information about the frequency and number of occurrences of problems and can help with prioritization when deciding which problems to address first.

Linked RFCs. Reference to RFCs that have been requested in order to resolve a problem should be recorded in the problem record. This provides a useful record of successful or unsuccessful changes that can be analyzed in the future for a more efficient resolution to similar problems. The results of the changes should be fed back into change reviews.

Date and time stamps. An accurate record of when the problem was first recorded, when updates occurred, and when it was closed will ensure that effective analysis and reporting can be carried out.

A target response time may be recorded for when the next activity on the problem must be completed. This can prove to be a valuable metric when assessing the performance of the problem management team against service level agreements (SLAs) and customer satisfaction.

Problem details. Accurate details describing the problem should be recorded, providing as much information about the problem as possible, including details of the configuration items (CIs) within the infrastructure that are affected.

Problem category. Each problem should be assigned a category such as Hardware, Software, Network, Process Failure, or Training Issue. Categories are used to assist prioritization and for reporting and analysis purposes.

Note: Certain problem management tools can automatically link the categorization selection to a service level agreement (SLA) and can also be used to link to a specific service level as documented within the SLA.

Priority. The problem needs to be assigned a priority and this should be based on the assessment of the business impact and the time frame during which the problem must be resolved in order to minimize further disruption.

Table 3. Impact Versus Urgency Matrix

	Low	3	4	5
Urgency	Medium	2	3	4
	High	1	2	3
		High	Medium	Low

Impact

The above impact versus urgency matrix is just one method that can be used to help in determining the Priority to be assigned to the problem.

For example, if a pension company experiences a problem relating to the failure of funds transfers for all its pension holders that is caused by a faulty component that is difficult to find a replacement for, this might be determined as a high impact and a high urgency priority, particularly if the window of opportunity to perform the transfer is within a small finite period (typically pension fund payouts occur at the end of a month).

The failure of the funds transfer could have a very damaging effect on the company's credibility, as well as severely disrupting the finances of any pension holders expecting funds on this day. Also, it would be common for the financial institution to incur compensation or other financial penalties. The problem would therefore be assigned as a Priority One.

On the other hand, if the problem is discovered early in the month, this would still be considered a high impact problem, but with a whole month to find and install a replacement component, the issue might be determined a low urgency. In this instance the problem would be assigned a Priority Three.

Other factors that should be considered when assigning a priority include:

- The availability of resources or specialist skills.
- The size, scope, and complexity of the problem.
- Agreed service levels as these may dictate the order in which problems are addressed.
- The costs to the business of resolving or not resolving the problem.

These considerations should be used to allocate staff resources according to the priority of the identified problems, ensuring that resources are being directed toward solving the most critical difficulties.

Services covered and SLAs affected. The services and any corresponding agreed service levels that will be potentially impacted by a problem need to be indicated on the problem record. These are required in order to correctly classify and prioritize the problem. Service levels may be documented within service level agreements (SLAs), operating level agreements (OLAs), and underpinning contracts (UCs), or be internal targets documented as part of mission statements or improvement plans.

Links to further information. Typically, problems can be complex and require detailed documentation to help explain the nature of the problem to other support staff. Any associated documents that describe details of the problems, such as diagrams and proposals, should be stored and the location made known and linked to the problem record.

Note: Some available tools have functionality that enables association with additional documentation. This allows automatic launching of the documents when selected from within the problem record. This saves valuable search time for support teams and ensures that they can access the correct information when required.

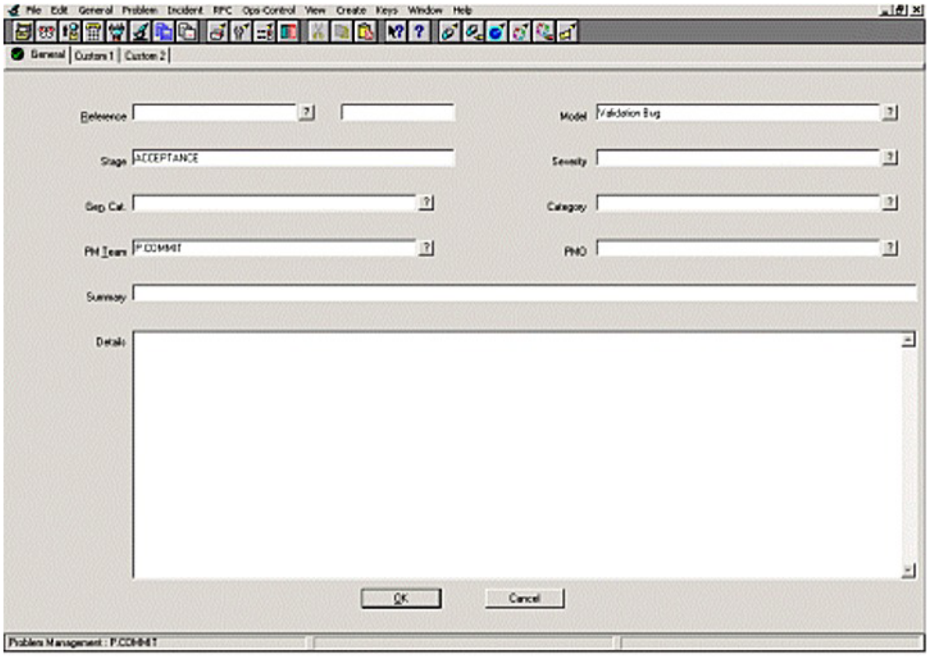
History. An accurate record of any investigation or support activity undertaken by the problem support or specialist support staff should be stored within the problem record. This can be used to determine the status of the problem should a customer enquire. It can also provide useful knowledge to specialist support staff in determining what activity has already been undertaken.

Status. The current status of the problem should be recorded in the problem record. The range of problem status codes could include:

- Recorded
- Under investigation
- Known error
- Resolved
- Closed

Workarounds. Any details of currently established workarounds should be detailed in the problem record. In addition, the location of any supporting documentation or procedural changes should be identified.

Permanent solutions. Once a solution has been determined for this problem, the details of how to apply this permanent fix should be recorded in the problem record. This information should be used to resolve the problem if it recurs in the future.



Model	Validation Bug
Stage	ACCEPTANCE
PM Team	P.COMMIT

Problem Management : P.COMMIT

Figure 4

Example of a problem record template

The above example shows a typical basic problem record template. Current and historical problem records should be stored within a problem database, ideally integrated with the service desk tool and the configuration management database. The ability to link incident records to problems and known errors records greatly enhances the ease of analysis and reporting.

The manner in which records are linked is determined by the functional capabilities of the chosen problem management tool set. Records of problems should carry links to incidents with matching symptoms or identical occurrences in order to aid the support analysts when investigating the problem.

Problem Investigation and Diagnosis

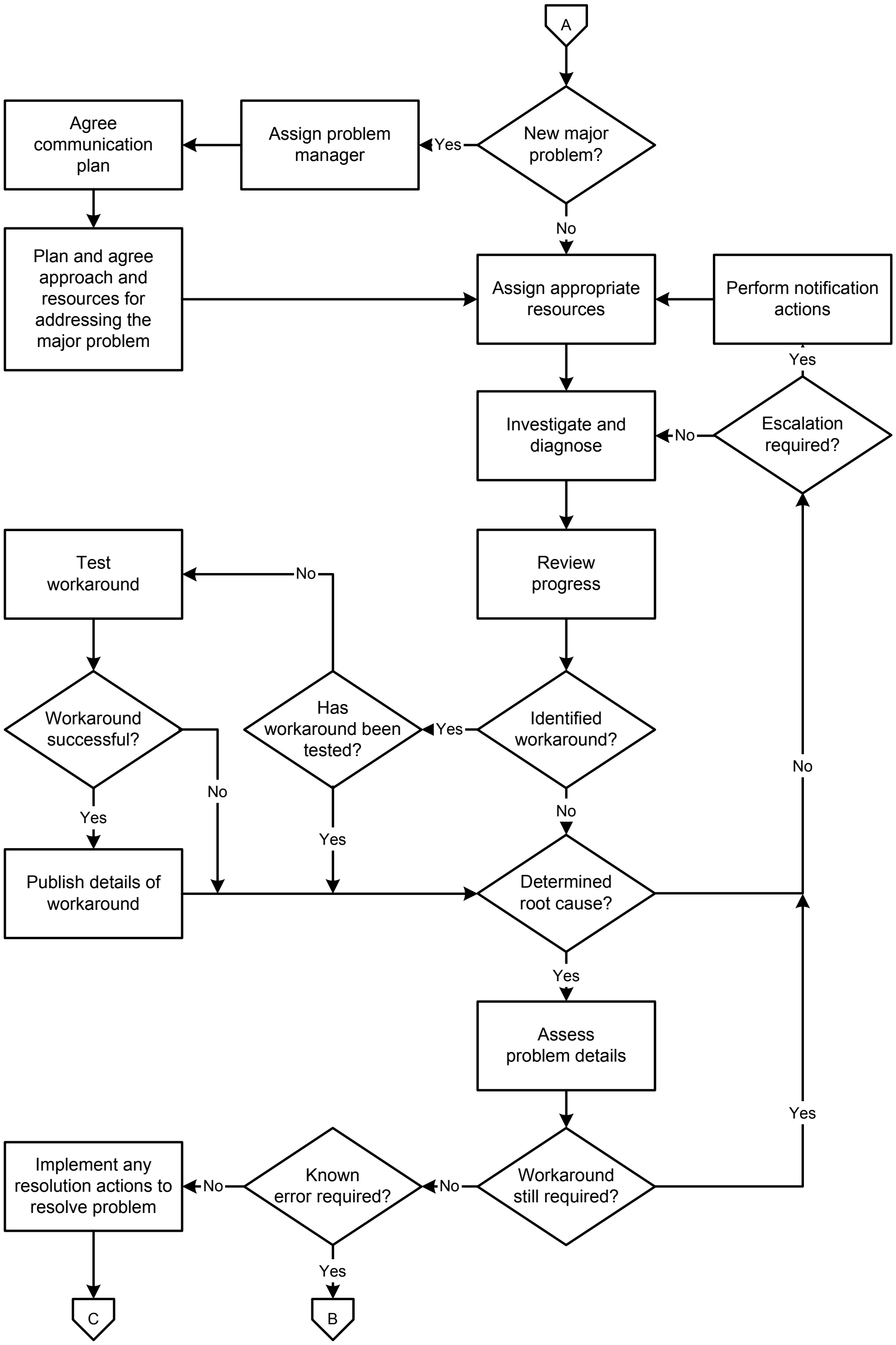


Figure 5

Problem investigation process flow chart

Normal and Major Problems

A major problem can be defined as a problem with a high impact or potentially high impact, which requires a response that is above and beyond that given to “normal” problems. (A normal problem will have less impact or potentially less impact to the business and may be assigned to individual problem support staff or resolution groups to investigate.)

Normally, longer timescales are available in which to plan a resolution to a major problem compared to a major incident (which often requires an immediate response). This means that it is better to treat the issue as a proactive requirement and manage it as a major problem. If left to incident management, because it lacks the immediacy of other incidents, there is a risk of it not being progressed. (An example of a past major problem is the year 2000 issue.)

Handling of Major Problems

A major problem should have assigned to it a specific problem manager who is responsible for co-coordinating all the support effort required to resolve the problem.

The problem manager should agree to a communications plan for informing affected parties, management, and support staff of the status of a major problem as it progresses through its life cycle.

During major problems, the handling of communications can often become a significant drain on resources and therefore be a major issue in its own right. The objective of the communications plan is to coordinate all communications during the life of the problem, ensuring that people affected by the problem are kept informed of the status of the problem and that managers and support staff are updated on its progress.

The communications plan should be owned by the problem manager and discussed and updated at regular intervals. Typically the plan should cover:

- A comprehensive list of key contacts who need to be regularly updated with status information.
- A comprehensive list of primary contacts who will act as onward focal points for information distribution.
- Contact details for all parties requiring updates.
- The different types of updates that will be required. Different update messages may be required, depending on the audience receiving the communication:
    - Senior management update
    - Update for all staff

  - Update for customers and business partners
  - Update for staff working on the problem
  - Press/media statement where required
  - Update for emergency services/authorities
- How often each type of update is required and when the next one is due.
- Who is authorized to release each different update statement.
- The mechanism by which each update will be communicated.

A template communication plan and suitable e-mail distribution lists should be developed for use during major problems. An example communication plan matrix is included as an appendix of this document.

The assigned problem manager should plan how to approach the problem and what resources to deploy. This may need to be done in consultation with senior managers and budget holders in order to gain the necessary approval. Customers might also be heavily involved in this decision-making process. Initiating a formal project might be the best approach to resolving complex problems, where budgets and time frames allow.

Once the communications plan, method of approach, and required resources have been determined, then any additional resources not already working on the issue should be deployed. All resources should have access to the problem record and the project plan (if one has been created), so that they can see what has been done so far and what actions both they and other resources should be working on now.

Assigning Normal Problems

Problem support staff members are responsible for owning normal, "non-major" problems and either progressing the problems themselves, assigning them to an appropriate resolver group, or putting together a virtual team containing members from different skill areas to work once a problem is assigned to a resolver group or virtual team, the team should start to investigate and diagnose the problem, in accordance with the problem's priority.

Problem support staff should monitor and track the problem records to ensure that they are being updated and that progress is being made.

Evidence

While investigating problems, you may find that there are instances when evidence of the root cause needs to be held securely for future reference. In the event of serious breaches of security, traces and event logs or any other important data depicting events should be retained and held in a secure area. This needs to be in a location where it can be located and accessed by authorized staff working on the problem. Evidence, especially involving malicious intent, should be secured from unauthorized access to prevent tampering or destruction. Storage should also conform to all confidentiality agreements, data protection, and other legislative requirements relevant to the information and its geographical location.

In cases involving theft or malicious intent, it may be necessary to preserve one or more CIs in their resultant state so that they can be used as evidence in any legal or disciplinary proceedings. These CIs need to be isolated and secured to prevent tampering or destruction of evidence. Continuity plans may need to be invoked in order to take the CIs out of service.

When diagnosing a problem, support staff should attempt to replicate it. This results in confidence that the problem has been fully identified. Documenting the steps taken to arrive at this point ensures that all staff involved is working to fix the same issue and can accurately test when a resolution is thought to have been achieved.

During the investigation and diagnostics process, problem management attempts to determine the root cause of the problem. Staff assigned should begin the investigation process by analyzing the service disruption in as much detail as possible.

A comprehensive review of any documentation (including the CMDB) connected with the configuration items involved should prove a valuable source of information and may provide details on configuration settings, operational guidelines, and troubleshooting procedures. The assigned support staff should look to identify:

- All of the configuration items that have been or are likely to be affected.
- Similar incidents that have been previously recorded.
- Any existing documentation provided by other SMFs, such as the service desk and incident management, concerning the problem.
- Which customers are affected by the problem: Is it an individual, group, site, or enterprise-wide? This information should be drawn from the CMDB if this is available.

- Any steps that have already been taken by incident management or specialist support teams to restore service or resolve the incident.
- Background information from customers. Customers often have valuable information concerning a service outage that is often overlooked.
- Any other relevant data that is available.

The objectives of problem investigation frequently conflict with those of incident resolution. For example, problem investigation may require detailed diagnostic data, which is available only when an incident has occurred; capturing this data, however, may significantly delay the restoration of service.

Close liaison between problem, incident, and change management needs to occur, so as to ensure that, when necessary, adequate time can be allocated to the collection of evidence. A judgment needs to be made as to whether a delay in restoration to collect diagnostics will be time well spent in the long run. Problem support staff should make this decision based on consultation with specialist support staff.

As a general rule, on first occurrence, an incident should normally be resolved as quickly as possible, unless it occurs outside normal service hours. Once service has been restored, diagnostic evidence can still be gathered. If, however, it is found that diagnostic evidence cannot be gathered following restoration, then on the second occurrence, a delay to collect diagnostics is normally preferable compared to the threat of continual repeat incidents. The exceptions to this are when the second occurrence takes place during a peak period, or when service level objectives may be breached by the delay. In the first case, support staff may have to wait for a recurrence during a quieter period; in the latter case, problem support staff should liaise with the business to agree an approach.

The following aspects are worth remembering in relation to the efficient handling of problems:

- The categorization of incidents can be an important first step toward problem definition. Problem management therefore benefits from close liaison with incident management, with regard to establishing common categories. This use of common categories greatly helps in the analysis of problems and facilitates better reporting.
- When assembling the correct resources to address problems, the skills of the team should be carefully considered and, if necessary, problem support staff should establish a

multidisciplinary team. Problem support should retain ownership and coordinate the work of this virtual team.

- Ensure that the support specialists involved have adequate tools and diagnostic aids in order to carry out their tasks effectively.
- Investigation procedures require that documentation on all products in the IT infrastructure be available to the support staff for reference purposes. This includes documentation on all aspects of the IT infrastructure that are deployed as part of the service delivery to the business.
- In addition to product information, it is also necessary to have effective procedures for the accurate collection of diagnostic data that can be used for problem resolution. Inappropriate use of data gathering procedures during an incident can delay the resumption of normal IT services and undermine the problem management process. It is particularly important that all support staff are not only familiar with these procedures, but have the skills and knowledge to use them effectively.

During incident and problem investigations, problem management staff members often require access to details of change requests. Recent changes are a common cause of incidents and problems affecting a business. The following diagram shows the typical cycle of events that the effective deployment of MOF SMFs seeks to break.

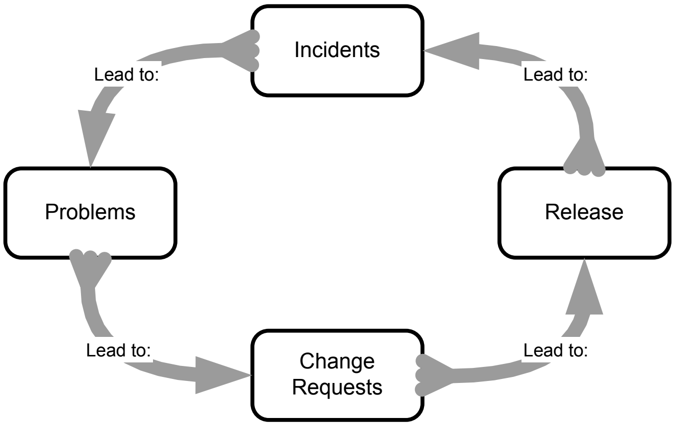


Figure 6
Problem event cycle

Problem management can often require a significant amount of effort from problem support staff and may need very technical resources to ultimately resolve problems. This can prove to be very expensive. The organization might decide that the efforts and costs are not justifiable, especially if there is an established workaround that can be lived with.

Note: Many diagnostic tools currently exist on the market to assist with the diagnosis of IT infrastructure problems. Most can either be described as one of two types:

- Software tools and utilities
- Hardware tools and utilities

Software driven tools include industry-standard suites of support tools that are designed to provide real-time understanding of the workings of the infrastructure. Other utilities often built into operating systems include:

- Event log files
- Monitors
- Trace programs

Hardware tools can come in the guise of specialist equipment designed with specific capabilities, such as network sniffers and trace equipment. Electronic diagnostic tools that interface with IT components and diagnose faults are also common.

Local or remote diagnostics can often be performed. Additionally, many hardware vendors include their own custom set of diagnostic tools with their products.

Problem Analysis Techniques

Problem management uses a number of techniques to assist in root cause analysis and the diagnosis of problems. When problem support staff members are initially tasked with resolving problems, it can sometimes be extremely difficult to know exactly where to start. This can be especially true when the problem is first reported. Initially, it is common for the customer to describe the symptoms of the problem, but this may not provide sufficient information to determine where to start searching for the root cause.

The use of problem analysis techniques identifies the key areas to be investigated and helps prioritize the investigative activities. Some of these techniques, such as the Ishikawa method (which follows a diagrammatical format), help educate users or customers as to the complexity of the problem. Seeing a picture of the problem displayed in this way is an excellent method for managing the expectations of customers and senior managers, as well as introducing specialist support staff to the size and complexity of the problem being addressed

Problem Restatement

Problem restatement is a technique that examines the problem through a continual refining of the problem statement by all involved, resulting in a clear understanding of the nature of the problem. It is also used to ensure that support staff are working toward resolving the principal issue and are not distracted by other issues they come across along the way.

This technique ensures that problem management is working to resolve the “right problem.” For example, a problem may initially be identified as being “We have faulty batches of printer paper, which are causing numerous printer jams and stacking problems.” However, as investigation progresses, this problem may need to be restated as “Our printer paper, once delivered, is being stored in damp conditions, resulting in numerous printer jams and stacking problems.”

Kepner and Tregoe Method

Management consultants Charles Kepner and Benjamin Tregoe developed a useful method of analyzing problems. Kepner and Tregoe state that problem analysis should be a systematic process of problem solving and should take maximum advantage of knowledge and experience. This technique identifies a five-phased approach to problem analysis. The five phases can be listed as:

- Defining the problem.
- Describing the problem with regard to identity, location, time, and size.
- Establishing possible causes.
- Testing the most probable cause.
- Verifying the true cause.

Depending on time and available information, these phases can be realized to some extent. Even in situations where only a limited amount of information is available or time pressure is high, a structured approach to problem analysis should be adopted to improve the chances of success.

Defining the Problem

Because any investigation is based on the definition of the problem, this definition has to state precisely which deviation(s) from the agreed service levels have occurred. Often, during the definition of a problem, the most probable problem cause is already indicated. Care must be taken not to jump to conclusions that can cause the investigation to move in the wrong direction.

In practice, problem definition is often a difficult task because of a complicated IT infrastructure and non-transparent agreements on service levels.

Problem Description

The following questions should be asked to describe the problem, in other words, what the problem actually is:

- *Identity.* Which part of the service does not function well? What exactly is the problem?
- *Location*. Where within the infrastructure does the problem take place?
- *Time.* When did the problem begin to occur? How frequently has the problem occurred in the past?
- *Size.* What is the size of the problem? How many parts are affected?

The problem description should be determined based on the answers to these questions.

Establishing Possible Causes

The next step should be to investigate which similar parts in a similar environment are functioning properly. With this, an answer can be formulated to the question of which parts could be showing the same problem but are not. It should then be possible to search effectively for relevant differences in both situations. Furthermore, past changes, which could be the cause of these differences, should be identified. The list of differences and changes thus generated will most likely contain the cause of the problem. Attempts should be made to extract the possible causes from this list.

Testing the Most Probable Cause

Each possible cause should be assessed to determine whether it could be the cause of the problem's symptoms. In this way, some of the possible causes can be eliminated.

Verifying the True Cause

The remaining possible causes should be checked to see whether they are the source of the problem–for example, by implementing a change or replacing a part. Support staff should first address the possible causes that can be verified quickly and simply.

Ishikawa Diagrams

The Ishikawa diagram, also referred to as a cause-and-effect diagram, tree diagram, or fishbone diagram, displays the factors that affect a particular quality, characteristic, outcome, or problem. The diagram is named after its developer, Kaoru Ishikawa (1915-1989), a leader in Japanese quality control.

The Ishikawa diagram, like most quality tools, is a visualization and knowledge organization tool. Collecting the ideas of a group in a systematic way facilitates the understanding of the nature of the problem and aids in the ultimate diagnosis of the problem. Several software tools have been created for assisting in creating Ishikawa diagrams.

An Ishikawa diagram 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. Ishikawa diagrams can be posted in communal areas within organizations where they are accessible to managers, support groups, and others. Creating the diagram stimulates discussion and often leads to increased understanding of a complex problem.

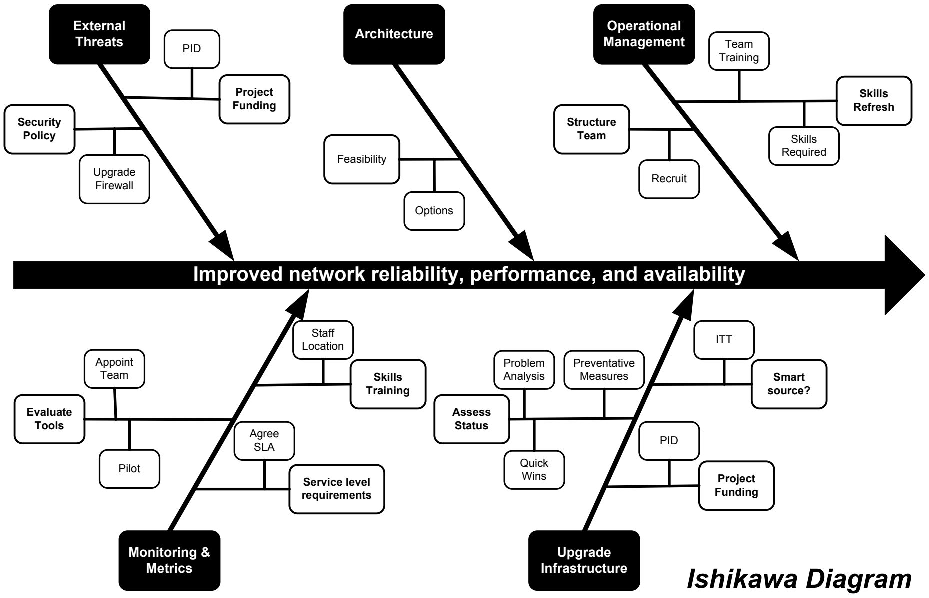


Figure 7

Example of an Ishikawa diagram

The Ishikawa diagram above was created to identify and prioritize the activities necessary to improve the overall reliability, performance, and availability of a problematic and unreliable network. The center arrow depicts the main goal.

The diagram illustrates five primary factors (external threats, architecture, operational management, monitoring and metrics, and upgrade infrastructure) that must be resolved to achieve the main goal, with each primary factor having several sub branches to be considered.

This diagramming technique can be a useful tool to demonstrate the complexity of a problem to a customer or assembled team. It can also assist problem support staff when prioritizing or determining which elements of the problem to address first and by which team or staff member.

It also serves well as a measure of progress, as areas that have been resolved are struck from the diagram. Additionally, the diagram can assist in tackling problems that are deemed "far too big an issue to tackle" by breaking them down into manageable chunks.

Flow Diagrams

Flow diagrams can be used to depict the elements of an end-to-end service to clarify what elements are involved. Looking at each element in turn can lead to a systematic diagnosis of all elements involved in the service and can help prevent key components of the service being overlooked.

Sorting and Timelines

During problem analysis, it can be beneficial to sort the collected evidence into some sort of order or timeline. What at first might seem to be a collection of unconnected events or error messages may reveal a pattern when placed in timeline order.

Similarly, a group of apparently random failures occurring over a number of servers may, once sorted by server address, reveal that the problem is limited to servers on a particular network segment.

The use of sorting to reveal patterns within problem evidence can be an invaluable technique during problem analysis.

Reviewing Progress

The problem support staff is responsible for regularly reviewing progress on existing problems and identifying instances where progress has stalled and/or escalation is required.

Often resolution groups share their time between resolving incidents, investigating problems, and carrying out their other daily responsibilities. As the investigation and diagnosis of problems is a proactive activity compared to restoring service following incidents or meeting production deadlines, there is a danger that sufficient time will not be allocated to work on allocated problems. Problem support staff should monitor progress and ensure that problem investigation is being given the appropriate time and resources.

In instances where sufficient progress is not occurring, problem support staff should initiate management escalation by notifying a predetermined management team. Typically, this team should consist of senior IT managers, including the problem manager. The management team should discuss the problem and confirm the priority, resources, and time that should be allocated to it.

If at any stage problem support staff members feel that the problem should now be designated "major problem" status, they should contact the problem manager, who then becomes responsible for making this decision.

Workarounds

Workarounds can serve as a temporary measure to provide restoration of the service that has been affected or as a temporary improvement to the service while a more permanent solution is sought. All workarounds should be tested to determine their effectiveness and should be clearly documented so that they can be used by other support teams such as the service desk. Test environments should be available in order to test the proposed workarounds without causing disruption to the live environment. Once a workaround has been proven, it should be deployed in conjunction with change management.

Root Cause and Problem Assessment

When the root causes of a problem have been successfully determined and if no workaround has yet been found, the problem support staff needs to assess whether there is still a need to find a workaround. In instances where a permanent resolution can be put in place quickly, there may be no need to continue working on finding a workaround. In other cases where actually planning and implementing a permanent fix will take time or prove too expensive, then work to identify a suitable workaround should continue.

Problem support staff also needs to assess whether a known error record needs to be created.

Diagnosis frequently reveals that the cause of a problem is not an error in a configuration item (hardware, software, or document), but is a procedural issue. (That is, the documented procedure was correct but someone did not follow it correctly.) In instances where the resolution does not involve a change to a configuration item, and the problem once resolved is very unlikely to recur (for example, the problem is found to be the result of a combination of circumstances unlikely to occur again), then it is not necessary to create a known error record.

Basically, an element of common sense has to be used here. The aim is to capture all useful known error data, without clogging up the system with hundreds of records that will never be required. If it is felt that there is any chance of a recurrence, then a known error should be recorded. The majority of problems will result in the recording of a known error.

In cases where it is decided that no known error record is required, problem support should coordinate the planning and implementing of any resolution actions before progressing the problem into the “problem closure” phase. Where a known error record needs to be created, the problem should be progressed to the “error control” phase.

Note: Integration of problem management with other service management tools can offer many benefits, including the ability of each SMF to see information stored by other groups. Data contained within the CMDB can, for example, prove to be very valuable to problem management for gaining information about a particular configuration item or for gaining a better understanding of the problem by assessing which configuration items are likely to be impacted by the problem.

Problem management tool sets come in a variety of forms. Most, however, fall into one of three distinct packaging methods:

- Stand-alone, no integration with other tools.
- Purchased separately, but integrated with one or more companion software tools, such as configuration management and test tools. These may be from the same or from different vendors.
- Bundled with other software tools, usually consisting of a configuration management tool and change management tool from the same vendor.

Error Control

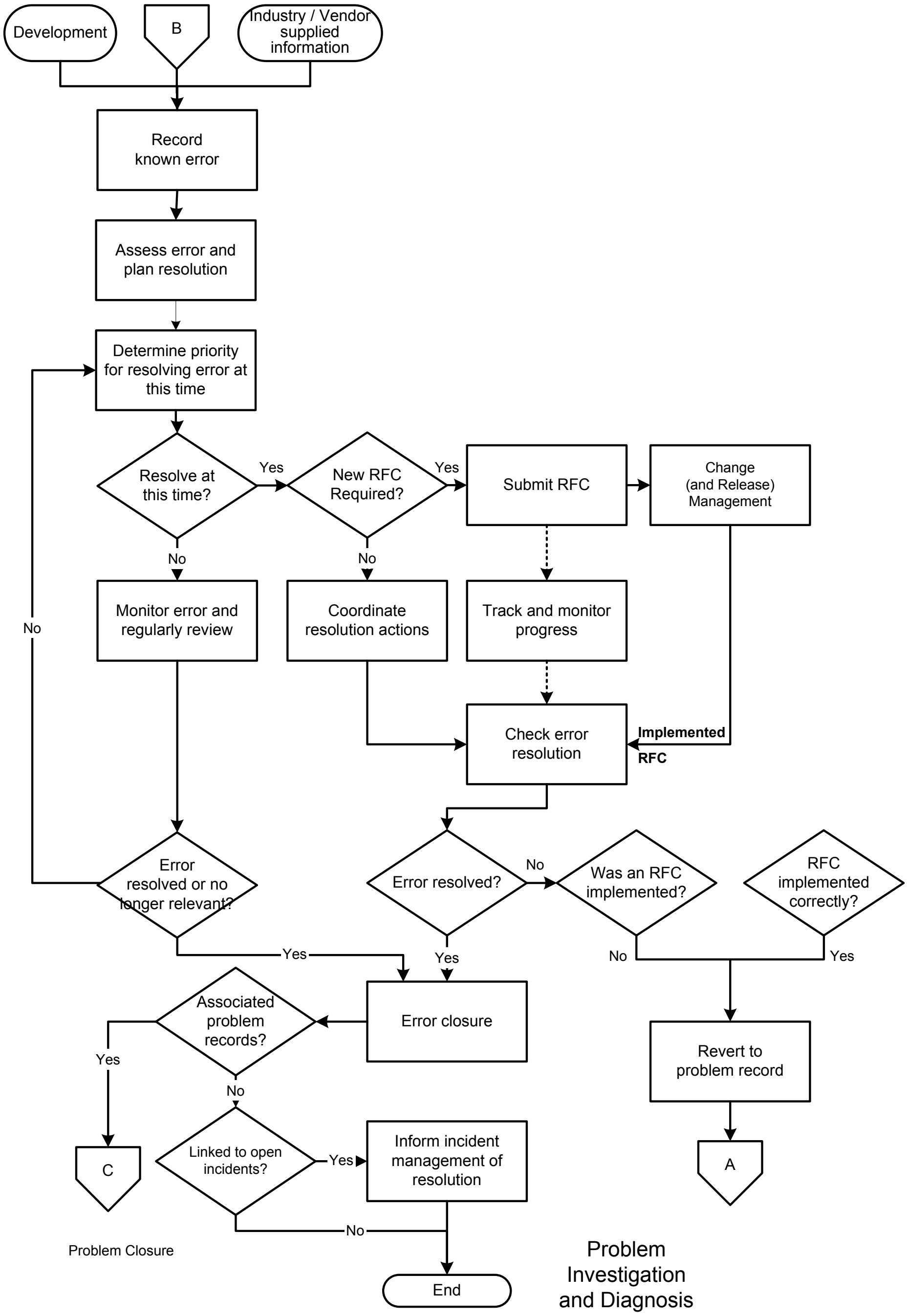

Development
B
Industry / Vendor supplied information
Record known error
Assess error and plan resolution
Determine priority for resolving error at this time
Resolve at this time?
Yes
New RFC Required?
Yes
Submit RFC
Change (and Release) Management
No
No
Monitor error and regularly review
Coordinate resolution actions
Track and monitor progress
No
Check error resolution
Implemented RFC
Error resolved or no longer relevant?
Error resolved?
No
Was an RFC implemented?
RFC implemented correctly?
Yes
Yes
No
Yes
Associated problem records?
Error closure
Revert to problem record
Yes
No
C
Linked to open incidents?
Yes
Inform incident management of resolution
A
No
Problem Closure
End
Problem Investigation and Diagnosis

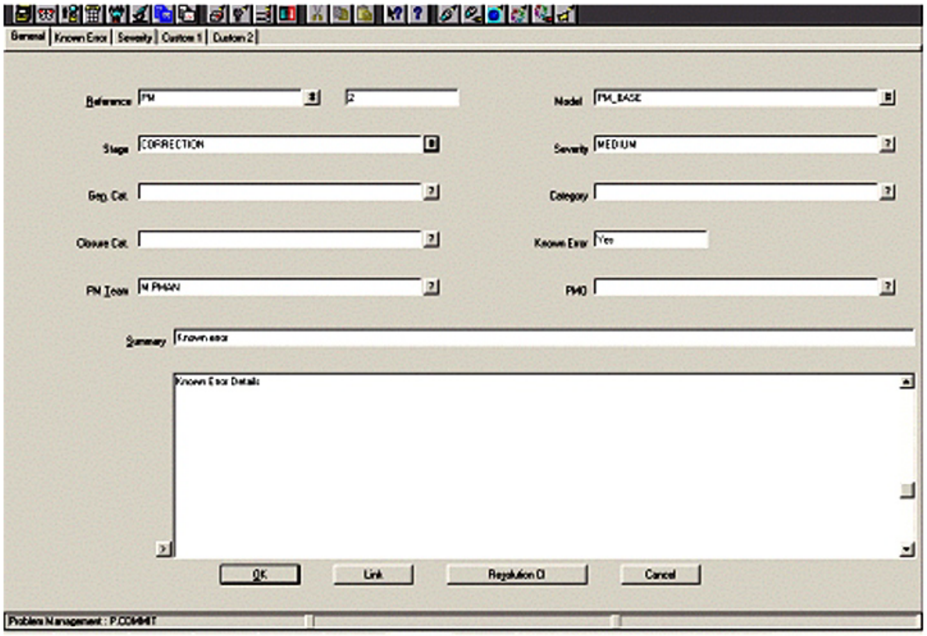
Figure 8

Error control process flow chart

Once a problem has been diagnosed and a resolution identified, if the resolution involves changing a configuration item (CI) or if there is any possibility of a recurrence, then a known error record should be created.

Known Errors

A known error is a problem that has been successfully diagnosed and for which a workaround has been identified. Therefore, a known error cannot be recorded until the root cause of the problem has been found. Additionally, one or more workarounds should be identified to allow circumvention of the problem.



Reference	PM 2	Model	PM_BASE
Stage	CORRECTION	Severity	MEDIUM
Grp. Cat.		Category	
Closure Cat.		Known Error	Yes
PM Team	M PHAN	PMO	

Summary: Known error

Known Error Details

Figure 9

Example of a known error template

Error Recording

The identification of known errors results from the investigation and diagnosis of any problems reported to the problem management team. Development teams will also identify problems while new software is being written or tested.

Suppliers can also provide valuable updates on known errors. This important data needs to be passed to the problem management staff responsible for recording and documenting all the information about these identified errors and ensuring that the resulting documentation is then updated.

All known error data should be stored securely, ideally within a database integrated with the service desk tool and the CMDB.

Known error records contain virtually the same fields as problem records, but should also include details of the identified resolution actions, any calculated costs for resolving the error, and the expected timescale for implementing the resolution. Incidents should be linked or otherwise associated with corresponding known error records in order for problem management to ascertain the impact that each error has on the organization.

Once the error has been recorded, the information can be used by the incident management process to identify workarounds and resolutions by matching incident symptoms against known errors. This information assists the support organization in resolving incidents in a timely and efficient fashion, preferably at first point of contact.

Error Assessment

Problem management should assess the error and determine which configuration items or processes need to be changed in order to resolve the issue permanently. Problem support staff are responsible for producing a plan for implementing the problem resolution.

In some cases, a temporary or permanent solution to the issue may be obvious; but in most cases, additional or specialist resources will be required to assess the known error and determine the best approach to a solution.

In these latter instances, problem support staff either assign the problem to an appropriate resolution group or assemble a virtual team with the required skills to plan an approach to resolving the error. Typically, problem support staff should assign an error in this way when:

- The complexity of the known error means the issue is clearly beyond the skills or capability of the problem support staff.
- There is insufficient data currently available from internal documentation and the CMDB that can be used by problem support to draw conclusions.

When a known error is assigned to a resolver group or virtual team, they should continue the error investigation and produce a resolution plan. Support staff will need access to such resources as:

- Information contained in the CMDB, including any appropriate service level agreements, problem records, related incidents, affected CIs, and affected users.
- Documented system procedures from manufacturers or suppliers.
- Any required third-party, supplier, or manufacturer resources.

However, any changes or additions to the known error record must be coordinated through the problem management contact responsible for resolving the known error. This ensures that this staff member remains completely informed about the status of the resolution activity. It also ensures that only pertinent information is recorded in the database.

Escalation to External Vendors

Suppliers should be called upon when known errors are identified with specific third-party supplied services or infrastructure components. In many cases, these components or services are covered by a UC, SLA, OLA, or warranty. As a general rule, the problem management staff should fully utilize any resources at their disposal or available to the organization in order to rectify each known error.

Escalation to external vendors may need to take place when:

- A resolution has not been found.
- The error lies within a vendor’s product.
- Internal support resources are limited.
- The required skills do not exist within the organization.
- Time frames do not permit a solution within the agreed service levels.

A detailed history of actions performed by any problem support personnel should be supplied to assist external vendors in determining a solution. This information should be present in the problem/known error records. An accurate record of events, evidence, and support activity helps prevent duplication of efforts that have been previously performed or attempted.

Often vendors may request log files or system dumps to aid in identification and diagnosis. A record of all activity taken by the suppliers should also be stored in the problem record for later retrieval. When escalating known errors, the responsibility for tracking and resolving the known error remains with the problem management staff.

Problem management staff should retain ownership of known errors that vendors are working on, track and record their progress, and make sure that the vendor is given appropriate access and assistance, while ensuring that the organization’s security policies are not breached.

When an error requires escalation between support tiers or to external vendors, a clearly defined procedure should be followed, aimed at ensuring that an appropriate level of detail is captured and passed to the next level of support. The problem manager must have clearly defined escalation procedures to ensure this is done efficiently. The procedures should contain:

- The point at which escalation will be required according to the length of time that has elapsed or the complexity of the issue being addressed. This should normally be contained within the underpinning contract or service level agreement.

- A clear and concise description of the reported known error.
- Any error messages or issues that the customer has experienced or that have been witnessed by support staff.
- Any and all resolution techniques that the problem management staff have applied toward known error resolution and the results of each attempt, including a detailed history of the sequence of activity.
- All other documented material deemed relevant.
- Any diagnostic tools or methodologies used by the problem support team.

It is possible that the problem management function may need to work alongside the problem management functions of other organizations, such as external vendors and partners. In cases where an issue is being progressed as a problem within more than one organization, it is important that the problem owners within each organization establish regular contact and keep each other up-to-date with the progress.

Organizations should plan in advance for this eventuality by discussing with their strategic partners how their respective major incident, problem management, and business continuity plans will work together. In today's complex business world, most organizations have some reliance on links and partnerships with other organizations and so should seek to build maturity into these relationships by ensuring that their support and continuity processes allow the organizations to work together effectively during times of difficulty.

Determining Resolution Priority

When the error has been assessed, the resulting information assists the organization in deciding how or when to resolve the issue. It should be noted that not all known errors will be resolved. An organization may well decide to postpone resolving a particular issue until a later date.

The costs of performing the resolution and the impact of any changes on the provision of services should be considered. A cost benefit analysis might need to be conducted to gain authorization from management to proceed with any required changes.

Some typical reasons for not resolving a known error might include:

- Too costly a solution or costs outweighed by the delivered benefits.

- Not practical to develop a solution.
- Only causing minimal "pain" at the current time, so resources better used elsewhere.
- Insufficient budget left during the current financial year.
- Lack of skills available to resolve.
- The recommended solution carries inherent business risk.
- Very effective workaround currently established.
- Planned technology refresh will remove this problem in the future
- Infrastructure requirements are due to change as a new business direction is being approved.
- Application/service nearing the end of its life cycle.

In these cases, the workaround can be considered the permanent solution. However, for documentation purposes, the known error is not closed but remains outstanding for the purposes of future incident resolution.

Error Monitoring

A known error's priority for resolution may change over time, as other changes are made or further issues become apparent. For example, if a particular known error is only associated with a small number of very intermittent minor incidents, it may be decided to not resolve it at this time. However, if in the future these incidents become much more regular, it might then be decided that the "pain factor" is now sufficient to justify implementing a permanent resolution.

Problem support staff should monitor existing known errors and regularly review their resolution priority in view of any changes.

In addition, problem support staff should also monitor whether any of the known errors have now been resolved or are simply no longer relevant. Some known errors will be resolved by actions taken outside of the problem management process, such as a routine software rollout to a later version. Other known errors will reach a stage where they are no longer relevant to the organization, such as when a particular application is phased out of use. Any known errors identified as either resolved or no longer relevant should be progressed to closure.

Error Resolution

When it has been decided that the resolution of a known error should proceed, problem support staff should perform an assessment of the resolution plan. This should be done in close liaison with any assigned specialist support staff. If necessary, problem support staff should then complete change requests (RFCs) according to change management procedures.

In the majority of cases, one or more RFCs may be required, although there may be instances where the necessary RFC has already been raised, or where the change is outside the scope of the change management system.

The priority of the RFC is determined by the urgency and impact of the error on the business. The request for change reference number should be included in the known error record and vice versa in order to maintain a full audit trail. Some tools permit these records to be linked automatically.

RFCs should be progressed according to change management procedures to ensure that all changes are properly tested and authorized, as well as minimum disruption to service.

The final stages of error resolution include impact analysis, detailed assessment of the resolution action to be carried out, amendment of the item in error, and testing of the change. These all fall under the control of change management. In extreme circumstances, authorization and execution of an urgent resolution may be necessary.

Throughout the change management process, problem management should monitor the status of the known error and, if applicable, the workaround. If the problem continues to affect the customer or progresses to a more disruptive state, then the problem management staff should notify change management to increase the priority of any outstanding changes that are required.

The linking of records enables efficient tracking of the status of any currently associated incidents, problems, or changes. Ensuring that these links are in place (where functionality permits) should also ensure an effective audit trail for future reviews of the problem cycle.

Once any changes have been implemented, problem support staff should confirm whether the error have been successfully resolved. This may include carrying out tests themselves or checking with users who were experiencing the errors. This should be done in coordination with the change management post-implementation review (PIR).

In many cases, continued monitoring of the change must be conducted to ensure the resolution has achieved the desired results. An error is considered closed when the customer agrees that the resolution has met the applicable business requirements.

If investigation reveals that the error has not been resolved, then problem support should first double check that the changes have been implemented as expected. If it is found that the expected changes have not actually occurred, then they should be passed back to the change management process.

If it is found that the changes have occurred correctly but failed to resolve the known error as expected, then problem management and change management staff should consider whether the changes should be backed out. The decision to back out a change depends on individual circumstances. For example, if a later service pack has been applied to try to resolve an error, but does not, then it is probably worthwhile to remain on the later version as it will include fixes for other potential problems. On the other hand, if the change included reverting back to a previous version of a software package, but the error remained, then it would be worthwhile to back out the change and return to the later version, which typically will have improved functionality.

If the planned resolution actions have been carried out successfully but have not resolved the error, then it is possible that the diagnosed root cause is incorrect. Problem management should revert the error back to a problem record and then enter the problem investigation and diagnosis phase again.

Error Closure

Problem management is responsible for closing known errors. The known error record in the CMDB is updated to reflect that a permanent resolution has been implemented for the error.

If there is a problem record associated with the known error, then this should be closed following the process defined under “problem closure.” If there is no corresponding problem record, but instead there are one or more associated incident records, then details of the error resolution should be passed back to incident management in order for them to resolve and close the incidents.

Problem Closure

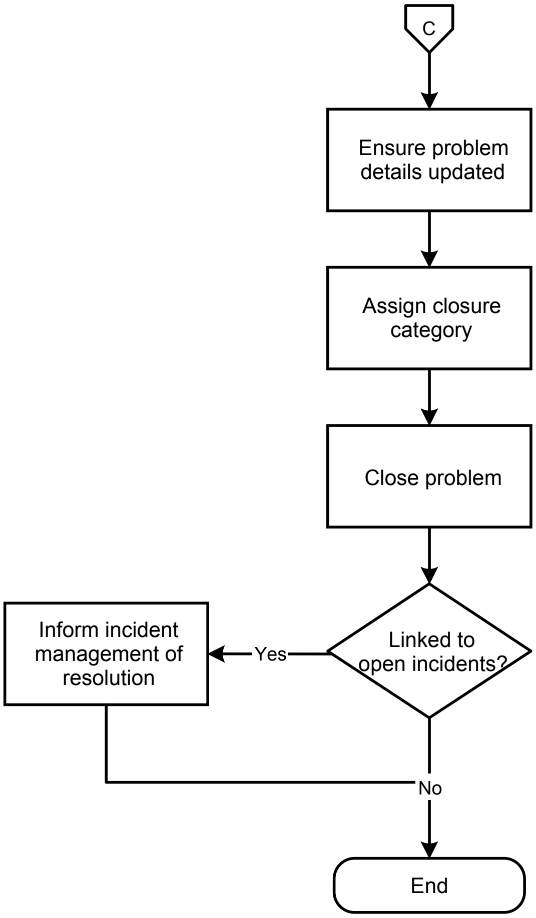

C
Ensure problem details updated
Assign closure category
Close problem
Linked to open incidents?
Yes
Inform incident management of resolution
No
End

Figure 10
Problem closure process flow chart

Problem records should be fully documented prior to closure, including details of all resolution activities performed and any workarounds that have been established.

Closure Categories and Codes

In addition to the initial classification of problems by category and priority, which can in themselves be a valuable source of information as to the types of problems being experienced, closure categories and codes should be used to provide additional information about the problem.

A closure category should be assigned to the problem, indicating the type of resolution action that was eventually taken. Examples include such things as “Software updated,” “Hardware replaced,” or “Procedure amended.”

Problems that are misdiagnosed and require subsequent re-classification should be recorded as such, to ensure that any such mistakes can be fed back to the support personnel or teams concerned. Problems can be closed with a closure code, which can be used to highlight the quality of how the problem has been handled.

For example, if the problem was classified correctly and then handled within agreed timescales, resulting in a successful solution, it could be closed with a code of A1. Problems that were misdiagnosed (thereby wasting time by being assigned to the wrong resolver group) but for which all else was handled well might be classified as B1. This coding should subsequently be used for reporting purposes to determine the quality of the problem management function.

Table 1. Example or Suggested Closure Codes

Closure Code	Call Handling Characteristic
A1	Problem classified and diagnosed correctly. Response/Fix timescales were met, and problem closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.
A2	Problem classified and diagnosed correctly. Response timescales were met, but Fix timescales were NOT met. Problem was closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.
A3	Problem classified and diagnosed correctly. Response/Fix timescales were NOT met, but problem closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.
A4	Problem classified and diagnosed correctly. Response/Fix timescales were NOT met, but problem closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.
B1	Problem classified and diagnosed incorrectly. Response/Fix timescales were met and problem closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.
B2	Problem classified and diagnosed incorrectly. Response/Fix timescales were Not met, and problem closed within agreed SLAs. Customer has not voiced any complaints and has agreed for problem to be closed.

The accuracy of problem reporting is dependent on the quality of information being stored in the problem records. If management reports are required and are being run based on the original classification, and subsequent closure does not correct earlier mistakes, then the accuracy of problem reports may be called into question.

Resolved problems can be closed and correctly classified once they are up-to-date. However, historical records should be maintained for use during trend analysis and reporting.

Once a problem has been closed, if it is associated with any open incidents, then incident management should be informed. The incident management process then handles the implementation of any outstanding actions to resolve the individual incidents, obtaining confirmation of resolution and then closure of the incident records.

Proactive Analysis and Review

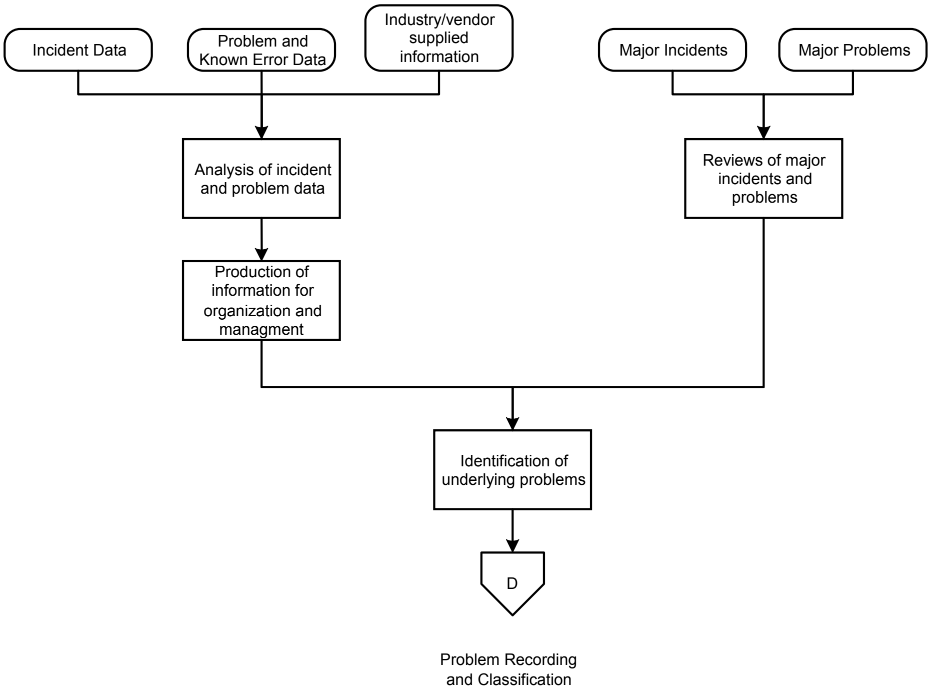

Incident Data
Problem and Known Error Data
Industry/vendor supplied information
Major Incidents
Major Problems
Analysis of incident and problem data
Reviews of major incidents and problems
Production of information for organization and managment
Identification of underlying problems
D
Problem Recording and Classification

Figure 11

Proactive analysis process flow chart

Proactive Analysis

The problem management SMF is responsible for analyzing incident, problem, and known error data to produce management information and identify underlying problems.

The objective is to be proactive by identifying areas where there is an increasing trend for a particular type of incident or problem. These trends should then be investigated and their root causes determined. The root causes should then be logged as problem records and resolutions found for them, so as to counter the worrying trends before they become major issues for the support organization.

The data analyzed by problem management may come from a number of sources: the service desk tool, problem databases, known error databases, and industry knowledge/external vendor-supplied information. The use of a single service desk tool with integrated problem and known error databases makes the task of collating all this data easier.

The problem management process should seek to identify trends within the historical incident data by considering these questions:

- Is the number of incidents of a particular type (category or sub category) increasing?
- Is the number of incidents assigned a particular closure category increasing?
- Is the number of incidents within a particular site or part of the infrastructure increasing?

Trends in these areas may indicate underlying infrastructure problems, increasing support requirements, the need for improved documentation, or specific customer training needs. Decreasing trends may indicate changing support requirements, dissatisfaction with the support service, or shortcutting of the incident management process. Not all trends indicate underlying problems, but problem management should attempt to understand why all trends are occurring.

Other trends that should also be questioned include:

- Is the number of unresolved incidents for a particular category or sub category increasing?
- Is the overall number of unresolved incidents increasing?
- Is the number of unresolved incidents assigned to a particular resolution group or individual increasing?
- Is the number of unresolved calls increasing within any particular tier of the support structure?
- Is the number of calls being resolved within particular resolution groups or tiers changing?

Trends in these areas may indicate changing support workloads and skills or resource shortages within resolution groups. Some of these trends can also indicate how well the incident management process and particularly the functional escalation element are working.

Another useful area to analyze is:

- The number of incidents being logged at each priority coding.
- The number of incidents being identified as “major incidents.”
- The number of incidents reaching high priority at some stage during their life cycle.

Trends in this area can reflect the performance of the problem management SMF in proactively identifying and resolving issues before they become high priority or major incidents. Organizations experiencing an increase in major incidents need to recognize this quickly and identify measures that can be put in place to counter this expensive trend.

Analysis of problem and known error data can make important contributions to the IT strategy and roadmap. If high impact problems or known errors exist with regard to a particular type of configuration item (CI), the replacement or upgrading of the CIs should be considered for inclusion in the strategy. A large number of lower impact problems on a particular CI type may mean that the future of the CI type needs to be evaluated.

Much of the information generated during proactive analysis will be of use outside of the problem management SMF. The problem management process should generate reports on a regular basis, including:

- Management reports on incident, problem, and known error numbers and trends for input into planning strategy and budget.
- Reports to the incident manager to help monitor the performance of the incident management process.
- Reports to the service desk manager to help monitor the performance of the service desk.
- Reports to service level management on the incidents, problems, and known errors recorded against specific services.
- Reports to managers responsible for resolver groups, indicating the workload and performance of each group.
- Reports to business managers showing the number and type of incidents logged from their area, the resolution times achieved, and the number of incidents still outstanding.

Note: To allow successful proactive analysis to be carried out by the problem management SMF, it is important to consider the functionality of the reporting tools available within the organization. Many service desk tools either have limited reporting capabilities or rely heavily on the use of additional third-party reporting tools. Frequently, the importance of the reporting capabilities is not considered when tools are initially purchased and this then seriously restricts the possibilities for proactive problem management.

If a service desk tool is based on a recognized mainstream database technology, and the vendor provides information on the database tables and their structures, then a number of third-party reporting tools can be utilized to develop and produce reports tailored to the organization's requirements.

Once any negative trends have been identified and verified, they should be logged as problem records for tracking purposes, and then problem management should work on determining the root cause and any corrective actions. The problem records should be classified and progressed following the normal problem management process.

Some reasons for trends will be obvious—for example, the number of incidents on a particular software CI increasing because it is currently being rolled out across the organization. Or, the number of calls being resolved is decreasing, which may require significant investigation. Only by understanding why these trends are occurring can problem management provide proactive information to management and other SMFs. Priority should be given to investigating the most worrying trends first.

Reviews

Problem management is also responsible for facilitating post-resolution reviews of all major incidents and major problems. These reviews focus on why the issues occurred, how well they were handled, and how they can be prevented in the future. Although the two types of review are similar, they have slightly different focuses, as detailed in the sections below.

Given that major incidents and major problems tend to be "expensive" events in terms of disruption, customer satisfaction, negative publicity, and the resources required to resolve them, the time taken to review these events in order to prevent recurrence or improve handling if recurrence does occur is time well-spent.

Major Incident Reviews

Major incident reviews should be carried out once it is certain that the incident has been resolved and business processes are back to normal operation. It is often advisable to allow a short cooling off period before holding the review. This allows participants time to put things into perspective, without being so long that events and actions are forgotten.

Problem management should collect and collate any documentary evidence from the incident as soon as possible, in advance of the review. The review should be scheduled and participants from all parties (including customers and third parties) invited to attend. In high profile instances where external organizations are involved, it may be appropriate to have an independent body facilitate and report on the review, so as to ensure impartiality and an unbiased view.

In preparation for the review, problem management should prepare a timeline showing the events and actions that took place according to the documentary evidence. This information should be circulated to attendees prior to the review meeting.

The agenda for a major incident review should include:

1. Introduction of attendees.
2. Brief introduction as to why the review is being held and what the objectives are.
3. Walk through the timeline for the incident, discussing the events and actions that took place. Document any additional events and actions that were not originally captured. Postpone any issues or disputes over "what should have been done," so that these can be returned to later.
4. Discuss why the incident occurred in the first place. What were the root causes? Is a recurrence likely and, if so, what can be done to prevent it? Document any actions identified.
5. Was the issue spotted soon enough? Could it have been recognized sooner? Was it flagged as a major incident soon enough? Document any actions identified.
6. How could the handling have been improved? How well did the restoration plan work? What was not done well? What worked well and should be remembered for the future? Was the response fast enough? Document any actions identified.
7. How well did communications and the communications plan work?
8. Go over the list of identified actions and identify owners and timescales. Explain how actions will be tracked and updated.
9. Close the meeting and thank all parties for their participation.

A management report should be produced detailing the findings of the major incident review. This report should be distributed to senior management.

Underlying issues and corrective actions identified during the major incident review should be recorded and tracked by problem management. It is important that problem management have the authority and management backing to ensure that the corrective actions are progressed by all parties.

Major Problem Reviews

Major problems should be reviewed in a similar fashion to major incidents. However, while major incident reviews tend to be very timeline focused, looking at the speed of detection, escalation, and resolution, major problem reviews tend to be less time-focused and should instead concentrate on the success of the planning and resourcing.

The review should occur when it is certain that the problem has been resolved. Participants from all parties involved (including customers and third parties) should be invited to attend. In high profile instances where external organizations are involved, it may be appropriate to have an independent body facilitate and report on the review, so as to ensure impartiality and an unbiased view.

In preparation for the review, problem management should collate all available evidence and prepare a timeline showing the main events and actions that took place. This information should be circulated to attendees prior to the review meeting.

The agenda for a major problem review should include:

1. Introduction of attendees.
2. Brief introduction as to why the review is being held and what the objectives are.
3. Walk through the timeline for the problem, discussing the events and actions that took place. Document any additional events and actions that were not originally captured. Postpone any issues or disputes over "what should have been done," so that these can be returned to later.
4. Discuss why the problem occurred in the first place. What were the root causes? Is a recurrence likely and, if so, what can be done to prevent it? Document any actions identified.
5. Was the problem flagged as a major problem soon enough? Were appropriate resources and budget made available to work on the problem? Document any actions identified.
6. How could the planning and handling have been improved? What was not done well? What worked well and should be remembered for the future? What could be done better next time? Document any actions identified.
7. How well did communications and the communications plan work?
8. Go over the list of identified actions and identify owners and timescales. Explain how actions will be tracked and updated.
9. Close the meeting and thank all parties for their participation.

A management report should be produced detailing the findings of the major problem review. This report should be distributed to senior management.

Underlying issues and corrective actions identified during the major problem review should be recorded and tracked by problem management. It is important that problem management have the authority and management backing to ensure that the corrective actions are progressed.

Arbitration

The problem management function should provide an arbitration function within the IT organization. If the identify of the person or team progressing an issue, change, incident, or problem is unclear or is in dispute, the problem management function should talk to all parties concerned and decide where the responsibility lies.

Problem management needs to have support and commitment from senior management in order to carry out this role. Where issues involve external vendors and/or partners, problem management should arrange meetings to bring all parties together and then facilitate discussions.

Roles and Responsibilities

Principal roles and their associated responsibilities for the problem management process have been defined according to industry best practices. Organizations might need to combine some roles, depending on organizational size, organizational structure, and the underlying service level agreements existing between the IT department and the business it serves.

It is important to remember that these are roles rather than job descriptions.

The roles required within the incident management process are:

- Problem manager
- Problem support
- Specialist support

Problem Manager

The problem manager is responsible for continually driving forward the problem management function and is the owner of the problem management process. The problem manager is responsible for optimizing the process over time and should intervene when the process breaks down. To ensure that the full benefits of problem management are realized, it is vital that responsibility for problem management be allocated to personnel with the time and inclination to focus on the role. As problem management is largely a proactive function, the role should not be mixed with other roles that have reactive responsibilities, otherwise the reactive roles are likely to push problem management into the background.

The problem manager is responsible for coordinating the operation of the problem management process and ensuring that its objectives and goals are met. In a small organization with a simple IT infrastructure, the problem manager might do much of the "problem management." However, in larger, more complex organizations, a number of problem support roles are necessary in order to assist the problem manager. The problem manager should then delegate day-to-day activities to the problem support staff, while continuing to perform the process coordination, planning, and development tasks.

The problem manager role is responsible for allocating problem support staff to work on problems and conduct reviews following the resolution of major incidents or major problems.

In some instances, temporary problem managers may be appointed from other areas of the business if it is felt that they are well-placed to manage a particular problem. Account managers or business liaison managers are often suitable choices to perform this role.

Table 2. Problem Manager Responsibilities

Role	Main Responsibilities
Problem Manager	Developing and maintaining the problem management process Driving the efficiency and effectiveness of the problem management process Producing management information Managing problem support staff Allocating support resources Monitoring and improving error control Developing proactive problem management activities Coordinating the organization's response to major problems

Problem Support

The size of the staff performing problem support roles varies depending on the size of the organization and the complexity of the IT infrastructure. In small organizations with relatively simple IT infrastructures, the problem manager is likely to also perform the problem support role. In larger organizations, the problem manager coordinates a number of problem support staff. As the size and complexity of the organization increases, so does the number of problem support roles.

It is important to have sufficient resources in this area, otherwise organizations can easily reach a situation where there are enough problem support staff to identify corrective actions, but not enough to ensure that all recommendations are followed up.

Problem support staff should have a good knowledge of problem solving techniques and preferably a broad experience of the technologies in use within the organization. Problem support staff should guide and work alongside specialist support staff to investigate problems and identify solutions.

Table 3. Problem Support Responsibilities

Role	Main Responsibilities
Problem Support	Identifying and investigating problems Raising RFCs to clear errors Monitoring progress on resolving known errors Advising incident management staff Reviewing major incidents and major problems Guide and assist specialist support staff Identifying trends and potential problems Raising RFCs to prevent the recurrence of problems Preventing the replication of problems across multiple systems

Support Technicians (Specialist Support)

Microsoft Operations Framework divides the IT environment into a set of layers: Each layer depends upon a firm foundation in order to function effectively. For the IT department, these layers are:

- Service
- Application
- Middleware
- Operating system
- Hardware
- Local area network
- Facilities
- Egress

Each layer has a support technician role that is responsible for participating in a resolution group whenever that layer is experiencing an incident. They are also actively involved in identifying problems and known errors.

Many individual teams within the IT organization may become involved with resolving different types of problems and known errors. These “resolution groups” should each have a queue within the problem management tool, to which problems requiring their specialist knowledge are assigned. Not all resolution groups will be purely “technical” groups, but they can all be seen as performing some form of specialist support function. Examples of “non-technical” resolution groups might be procedural experts or teams that are responsible for training, processing RFCs, or dealing with requests to change agreed service levels. The staff members within these groups are performing specialist support roles. Not all specialist support staff is necessarily internal, as external vendors may form a number of the resolver groups.

Staff members performing problem support roles are unlikely to have an in-depth knowledge of all areas within the IT infrastructure, especially as new technologies continue to emerge. Staff members within specialist support roles are responsible for providing specialist knowledge in order to assist problem management in investigating and resolving problems.

When resolution actions are identified, specialist support staff should implement those actions under the control of the change and release management processes. Once resolution has been achieved, they should update the problem record and pass it back to problem support staff for closure.

Specialist support teams should also seek to identify underlying problems and notify problem management of the problems.

Table 4 - Support Technicians' Responsibilities

Role	Main Responsibilities
Application Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error
Middleware Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error

Role	Main Responsibilities
Storage Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error Executes end-user data restoration requests.
Print Support Technician	Ensures that sufficient hardware spares are on-hand to meet service level requirements Creates printer standards to minimize spare parts requirements Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error
Database Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error Executes end-user data restoration requests.

Role	Main Responsibilities
Directory Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error Executes end-user data restoration requests.
Operating Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error
Hardware Support Technician	Ensures that sufficient hardware spares are on-hand to meet service level requirements Manages the company's supply of spare parts Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error
Network Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error

Role	Main Responsibilities
Facilities Support Technician	Handling service requests Monitoring incident details, including the configuration items affected Incident and problem investigation and diagnosis (including resolution where possible) Detection of possible problems and the notification of problem management The resolution and recovery of assigned incidents Acting as a restoration team member if required during major incidents Carrying out actions in order to correct known error

Relationship to Other Processes

Service Desk

The service desk acts as the interface between the business and IT.

The service desk, with its responsibility for day-to-day coordination of the incident management process, is ideally placed to identify recurrent or multiple incidents that point toward an underlying problem. As such, the service desk is an important source of information for problem management.

In return, problem management works to identify and document workarounds and solutions that the service desk can utilize while performing initial support on new incidents.

When resolutions or workarounds are identified by problem management, the information is then passed to users by the service desk.

Problem management also aims to identify information that the service desk can utilize to proactively advise users. In the long run, effective problem management should reduce the number of incidents being reported to the service desk.

Incident Management

Incident and problem management are closely related but have very different focuses within the support organization.

While incident management is focused on restoring normal service as quickly as possible, problem management is focused on the identification and resolution of underlying problems and their root causes.

Incident management provides problem management with much of the information it requires in order to identify the existence of underlying problems. Problem management analyzes incident statistics to identify the occurrence of multiple incidents or increasing trends for specific types of incidents.

In return, problem management seeks to resolve the underlying causes of these incidents, so as to prevent their recurrence.

Problem management also maintains information about existing problems and known errors, including known workarounds and solutions. Incident management makes use of this information to provide a quick resolution of incidents.

Problem management is also responsible for reviewing major incidents once they have been resolved. During these reviews, the aim is to identify underlying causes so as to prevent any recurrence, to identify triggers that can be used to give early warning of any recurrence, and to identify how well the incident was handled so as to improve future reactions.

Change Management

When problem management identifies resolution actions that require changes to configuration items, these changes are implemented under the control of the change management process.

The control provided by the change management process reduces the amount of changes that have to be backed out and ensures that backout plans have been documented in case they are required. The coordinated testing of changes reduces the chance of subsequent incidents caused by the implementation of changes.

Change management also provides problem management with useful information on recent changes, the configuration items affected, and the reason for the changes.

Configuration Management

Configuration management provides vital information that is used during the problem management process. The CMDB contains information used to:

- Provide information on CIs.
- Assist with the classification of problems and known errors by indicating services and SLAs impacted by the failure of particular CIs.
- Identify the relationship and dependencies between CIs.
- Identify identical or similar CIs for comparison purposes and to prevent problem replication.
- Identify alternative routes and workarounds.
- Record changes to configuration items as a result of RFCs.

Release Management

Some resolution actions identified by problem management require changes that need to be incorporated and rolled out as releases. These releases are coordinated and managed by the release management process. In order to confirm that the expected resolution has occurred, problem management assesses the release in the production environment to validate that the known error(s) have been permanently fixed.

In a similar way to change management, release management provides the planning, testing, and coordination to roll out these releases without the changes resulting in further incidents.

Capacity Management

The capacity management process identifies capacity-related problems and flags these to problem management.

Problem management often works with the capacity management process in order to plan resolutions for capacity-related problems.

Financial Management

Financial management assists problem management with identifying the costs associated with resolving known errors, as well as not resolving those errors.

As such, the financial management process is a vital source of information for error control, allowing informed decisions to be made when and if an error should be fixed.

Availability Management

The availability management process works with problem management to propose solutions for the resolution of availability-related problems. Availability management may identify and report availability-related problems to problem management. Additionally, the process assists with the prioritization of problems and known errors by providing information on the cost of loss of availability.

Service Continuity Management

Service continuity management works alongside problem management to propose solutions for the resolution of continuity-related problems. Problem management assists service continuity management with the justification and prioritization of resolution actions. Service continuity management may also report continuity-related problems to problem management.

Security Administration

The security administration function assists problem management by proposing solutions for the resolution of security-related problems. Problem management assists security administration with the justification and prioritization of resolution actions. Service continuity management may also report security-related problems to problem management.

Network Administration

The network administration function assists problem management by proposing solutions for the resolution of complex network-related problems. Problem management assists network administration with the justification and prioritization of resolution actions.

Network administration may also report network-related problems to problem management.

Service Monitoring and Control

The service monitoring and control function is a source of information with regard to services and events that problem management can utilize during investigation and diagnosis of problems. Furthermore, the information can also be utilized during proactive analysis to identify underlying problems.

Directory Services Administration

The directory services administration function assists problem management by proposing solutions for the resolution of complex directory services-related problems. Problem management assists directory services administration with the justification and prioritization of resolution actions.

Directory services administration may also report directory services-related problems to problem management.

Storage Management

The storage management function assists problem management by proposing solutions for the resolution of storage management-related problems. Problem management assists storage management with the justification and prioritization of resolution actions. Storage management may also report storage-related problems to problem management.

Job Scheduling

The job scheduling function schedules the automatic running of any batch jobs required by problem management, such as reports or automatic escalation checks.

Print and Output Management

The print and output management function assists problem management by proposing solutions for the resolution of print and output-related problems. Problem management assists print and output management with the justification and prioritization of resolution actions. Print and output management may also report print and output-related problems to problem management.

Appendixes

Appendix A: Technologies Used

The screenshots used within this document are taken from Fox IT's Redbox service management application, which integrates the functions of configuration management, change management, service desk, incident management, problem management, and operations control to assist organizations in providing world-class support for their IT services.

Appendix B: Example Major Problem Communication Plan Matrix

Communication Plan Matrix					
Problem Number		Problem Manager		Date Plan Created	
Matrix Version Number		Date/Time Next Plan Review Due		Plan Last Updated	
Statement Type	Produced By	Statement (link to statement document)	Authorized By	Date/Time Issued	Next Due Date/ Time
Recipient Name	Organization	Contact Details	Update Type Required	Frequency	Method

Contributors

Many of the practices that this document describes are based on years of IT implementation experience by Accenture, Avanade, Microsoft Consulting Services, Fox IT, Hewlett-Packard Company, Lucent Technologies/NetworkCare Professional Services, and Unisys Corporation.

Microsoft gratefully acknowledges the generous assistance of these organizations in providing material for this document.

Program Management Team

William Bagley, Microsoft Corporation

Neil Battell, Fox IT

Lead Writers

Neil Battell, Fox IT

Tony Gannon, Fox IT

Contributing Writer

Dave Phillips, Compuware

Editors

Patricia Rytkonen, Volt Technical Services

Sybil Wood, Volt Technical Services

Other Contributors

Char LaBounty, LaBounty & Associates, Inc.

Steve McReynolds, Microsoft Corporation

Eric Stoever, Avanade, Inc.