

21.05.07

Deliverable DS3.15.1: In Service Support Structure



Deliverable DS3.15.1

Contractual Date: 31/01/07
Actual Date: 21/05/07
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: SA3
Work Item: Work Item 13
Nature of Deliverable: R
Dissemination Level: PU
Lead Partner: DANTE
Document Code: GN2-07-118v2

Authors: L. Kudarimoti (DANTE)

Abstract

This document is a general introduction to the Multi-Domain Monitoring (MDM) Service developed by GN2 JRA1, and Service Support. It also presents the motivation for providing support using the MDM Service, In Service Support (ISS) components and processes, and lists the NRENS involved in this project.

Table of Contents

0	Executive Summary	v
1	Introduction	1
2	In Service Support (ISS) Overview	2
2.1	Objectives	2
2.2	Users	2
2.3	Expected Software Deployments	2
2.4	Introduction to the ITIL Framework	3
3	In Service Support (ISS) Plans and Processes	5
3.1	Service Support - Processes and Functions	5
3.1.1	Service desk	6
3.1.2	Incident Management	8
3.1.3	Problem Management	12
3.1.4	Change Management	15
3.1.5	Release Management	16
3.1.6	Configuration Management	17
3.2	The Tools	17
3.2.1	CMDB and CMDB-lite	17
3.2.2	Trouble Ticket System	19
3.2.3	Problem management tool - Bugzilla	19
3.2.4	Deployment monitoring system	19
3.3	Use cases	20
3.3.1	Use case – 1: Incidents resulting in known-errors	20
3.3.2	Use case – 2: Incidents, unknown-errors and creation of work-arounds	22
3.3.3	Use case – 3: Incidents, unknown-errors and resolution using RFC	23
3.3.4	Use case – 4: Proactive incident and problem detection	24
3.3.5	Use case – 5: Introduction of a new product	25
3.4	Service Portfolios	26
3.4.1	Managed Service Support (Hardware and Software Support)	26
3.4.2	Software-only Support (Support restricted to a set of Applications)	27

4	NREN Participation	28
4.1	Incident Management and Service desk	28
4.1.1	Problem Management	28
4.1.2	Release Management	28
4.1.3	Change Management	29
4.1.4	Other	29
4.2	Current Status	29
5	Conclusions	30
6	References	31
7	Acronyms	32

Table of Figures

Figure 3.1:	The processes that make up the MDM Service Support Structure	6
Figure 3.2:	Service desk and its roles	8
Figure 3.3:	Illustration of communications between Incident Management and other entities	10
Figure 3.4:	Illustration of communications between problem management and other teams	12
Figure 3.5:	Flow chart illustrating use case 1- Incidents which are known errors	21
Figure 3.6:	Incident resulting in RFC being generated by the problem management team	22
Figure 3.7:	Flow chart illustrating change management procedures being followed	23
Figure 3.8:	Illustration of proactive incident and problem detection	24
Figure 3.9:	Flow chart illustrating Introduction of a new product	25

0 Executive Summary

The aim of GÉANT2 project is to provide new Information Technology services to its community of users. One of these services, called the Multi-Domain Monitoring Service (MDM Service), will support the detection and diagnosis of network related problems that span multiple network domains. The infrastructure required for this service is being implemented with the collaboration of the National Research and Educational Networks (NRENs) involved in this activity.

This document describes:

- How the required infrastructure is setup.
- The various processes involved, and how these processes will interact with users and with each other.

There are two main aspects to providing a service; service support and service delivery:

1. **Service Support** involves assisting the users of the products, and represents the operational aspect of the service.
2. **Service Delivery** deals with enhancing the service itself by regularly capturing and analysing the experiences and requirements of the users, as well as extending the service to new users and new products. This is the tactical side of providing a service.

As part of Service Delivery, Service Level Agreements (SLAs) will be drawn up based on the experience gained during the pilot and prototype phases. SLAs provide detailed information about the level of support that the users can expect from the service. The key objectives of all the processes in Service Delivery are to verify SLA adherence, continuously gather requirements, and on the whole improve the MDM service provisioning.

This document focuses on Service Support. However, Service Delivery is introduced in the concluding sections of the document.

This document consists of following sections:

- **1 Introduction:** A general introduction to the MDM service and Service Support. It also talks about the motivation for providing support using the MDM Service.
- **2. In Service Support (ISS) Overview:** An overview of ISS objectives and components.
- **3. In Service Support (ISS) Plans and Processes:** A description of In Service Support (ISS) and its methodologies. It also describes ISS objectives and target users, and the structure and processes that

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

will be defined in order to provide support for the MDM Service. This chapter also has Use Case based illustrations of how the supported structure will handle various scenarios expected in providing support.

- **4. NREN Participation:** This lists the parties involved in providing support.

1 Introduction

The GÉANT2 JRA1 activity on Multi-Domain Monitoring has been researching a framework that can be used to build software products to provide network monitoring across multiple domains. As a result, it has delivered many products that have been deployed in locations across the NREN community. More products are in development. These products and deployments not only prove the concept of multi-domain monitoring and the framework developed, but also suggest the possibility of providing a reliable platform for other services (such as Bandwidth reservation and technology testing) that require network monitoring.

However, in order to use these products in an operational environment they must be:

- Reliable
- Quality controlled
- Fully supported

Support involves addressing user questions, resolving user problems, and updating the software to provide enhancements and fixes to software errors. To achieve all this, a structure is required that defines the processes that will be followed by the support team in order to provide full user support.

This document describes the processes and interactions between the processes that will form the support structure of the MDM Service.

MDM Service has been designed with the knowledge that products from other activities will need to be supported in a similar fashion in the future. As such, the MDM Service structure should be applicable to other products and activities.

2 In Service Support (ISS) Overview

2.1 Objectives

The objectives of MDM Service Support are to provide:

- Organised, effective, user-friendly and timely support for users of products.
- Well-defined and efficient processes to provide support.
- Feedback gathering from users on the service provided.
- Regular reports on the level of service provided.
- Service Level Agreement with users - Definition and Monitoring.
- Continuous improvement to support processes.
- Service support extensible to new products.

2.2 Users

The following groups are potential users of the MDM Service:

- Network Operations Centre personnel who are interested in troubleshooting network issues that span multiple domains.
- Performance Enhancement and Response Team (PERT) who are interested in troubleshooting network performance related issues.
- NREN members who are interested in installing MDM supported software in order to export data, and also interested in analysing data across multiple networks.
- Special Projects and Researchers who require the capability to view network measurement data from multiple networks related to their projects.

2.3 Expected Software Deployments

The MDM Service will provide support to users in three phases:

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

- Pilot
- Prototype
- Operational

The Pilot and Prototype phase will have a controlled number of deployments and users, who will be supported by the MDM Service.

During the Pilot phase, 30 deployments are planned for the software supported by the MDM Service. This will include five NRENs and DANTE (who will deploy the software bundle supported by the MDM Service). This software bundle will include five different types of software.

During the Prototype phase, 108 deployments are planned for the software supported by the MDM Service. This will include eleven NRENs (including the five NRENs from the Pilot phase) and DANTE (who will deploy the software bundle supported by the MDM Service). This software bundle will include seven different types of software (including five from the Pilot phase).

For the Operational phase, requirements will be gathered during the Prototype phase from the entire user community listed in the previous section. These requirements will help the service in calculating the total number of deployments expected and the effort required to support these deployments. All NRENs interested in deploying the software will be supported.

2.4 Introduction to the ITIL Framework

The IT Infrastructure Library (ITIL) is a framework definition that specifies a set of processes and functions to be used for the management of any IT Service. These definitions are based on best practices gathered from public and private sector industries world wide. If an organisation wishes to adopt these specifications, the process definitions need to be tailored according to the constraints faced by that organisation.

The advantages of adopting such a framework are:

- It provides a best practices guide based on IT management principles that have a proven track record in the area of IT Service provisioning.
- It can help in standardized communications between various groups in the organisation that are collectively providing the service.
- It can help in establishing a common terminology to improve understanding between people within the same organisation, as well as with third-party providers required by the service.

ITIL is developed by the Office of Government Commerce (OGC), which is the office of the HM Treasury responsible for improving value for money by driving up standards. The processes in ITIL are supported by the British Standards Institution's standard for IT Service Management (BS15000). ITIL and IT Infrastructure Library are registered trademarks of the OGC.

For the above reasons, the ITIL framework has been adopted for the MDM Service. The processes defined and the terminologies used in the later sections of this document are derived from the processes defined in the ITIL framework. These processes have been adapted to suit the constraints of the MDM Service, such as resource availability, and organisationally and geographically distributed team members.

3 In Service Support (ISS) Plans and Processes

This section discusses the plans for setting up the support aspect of the Multi-Domain Monitoring Service. It explains the processes to be followed by the team members working on this activity. It also explains the interaction between these processes, and the stages in which these processes will be implemented.

A dedicated section on Tools summarizes the various tools that will be used by the support team (see 3.2 “The Tools”)

Use case illustrations of how these processes will work together are included (see 3.3 “Use cases”). These show how these processes will handle common scenarios, such as the user approaching the Service desk for support and the software being updated to fix problems

The final section describes the service portfolios that will be offered to the users. The software being supported by the MDM Service depends on other factors, such as hardware and Operating System. Each portfolio defines the level of support offered for all these factors.

3.1 Service Support - Processes and Functions

The processes and functions that form the Service Support for Multi-Domain Monitoring Service are illustrated in Figure 3.1 below.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

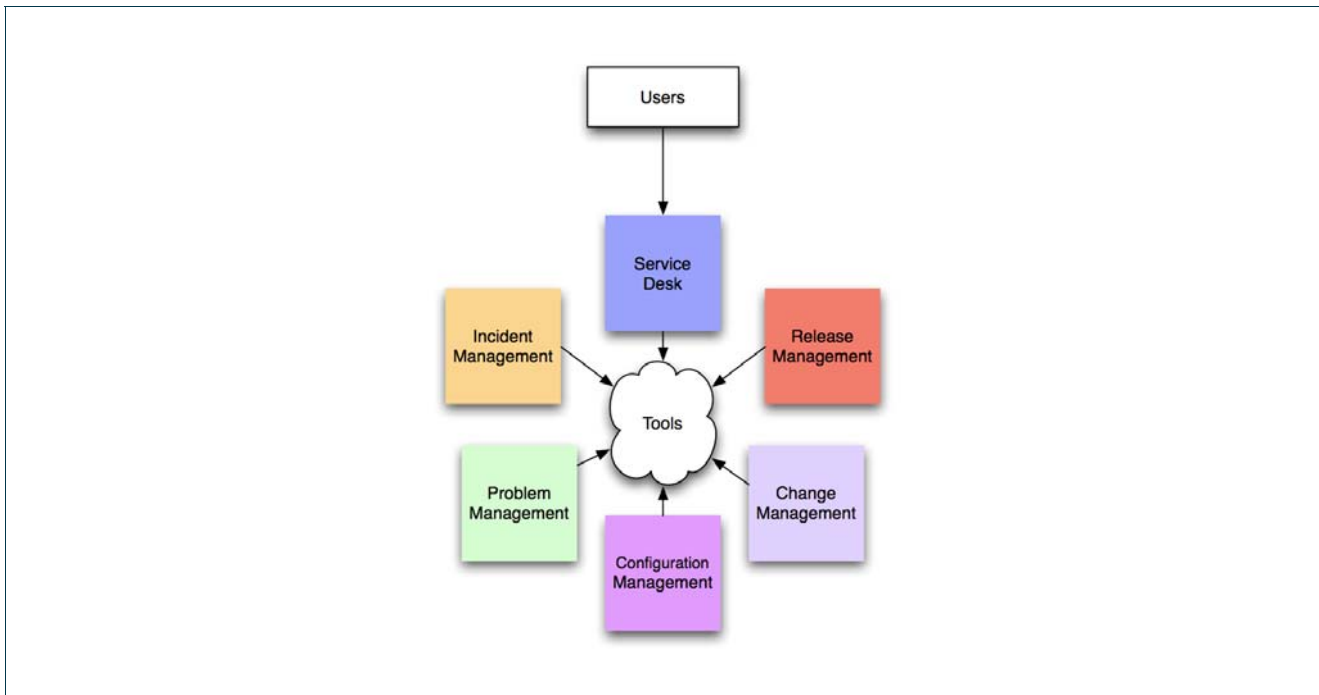


Figure 3.1: The processes that make up the MDM Service Support Structure

All these processes will be regularly improved according to user feedback and experience. The processes are designed to be simple during the initial phase of MDM Service, and will be enhanced continually. This is called a Continuous Service Improvement Program (CSIP).

The sections below describe the different processes.

3.1.1 Service desk

The Service desk will act as a Single Point of Contact (SPOC) for all communications with the users of the service. Apart from recording all the calls coming from users, the Service desk's main objectives are to:

- Deal directly with simple requests and complaints.
- Co-ordinate the restoration of normal operation of the supported software and thus contribute to the improvement of the MDM service.

The Service desk for the MDM Service is involved in all the processes defined in this section. The role of the Service desk in each of these processes is described within the sub-section dedicated to each process. Of all these processes, the Service desk's key role will be the incident management process, which is described in detail in the next section.

Whenever a call is received from users, the Service desk analyses it to discover if there has been any disruption to the expected operation of the supported IT infrastructure (software and hardware), or any

reduction in quality. Such disruptions or potential disruptions, or anything that results in reduced service quality, are registered as “incidents”. The Service desk retains ownership of such incidents at all times, and ensures that there is a rapid restoration of normal operation. The process of diagnosis, recording and investigating incidents and then finding resolutions, which can quickly restore normal operation, is called “Incident management”.

If the request is for general information, service enhancements or a complaint, the Service desk should acknowledge the request and then respond to it according to its priority. Although such requests usually carry less priority compared to incidents, the time and effort required to respond to these requests tend to be quite low. Providing a quick response will help maintain a positive image of the Service desk in the users’ eyes. Regardless of this, the Service desk’s highest priority will be to deal with incidents and follow the incident management processes.

All the processes defined in this section will use tools that will help them follow the defined processes. Because of the involvement of the Service desk in all the processes, it will maintain and use three tools, and use (but not maintain) one other tool. The three tools that the Service desk will maintain and use during the early stages of this activity are:

- A Trouble Ticket System for incident recording and incident management.
- A light weight Configuration Management DataBase (CMDB-lite), which will be used to manage the IT infrastructure configuration information.
- The existing deployment monitoring system, which helps the Service desk in proactively detecting incidents by sending alarms to the Service desk when it notices any problems with any of the deployed software.

The Service desk will also use the existing problem logging tool called Bugzilla. The problem and change management processes will, however, be maintaining this tool. More information about these tools and explanations of how they will be used are included in the sections below, and summarized in the later section on Tools.

Figure 3.2 illustrates the roles of the Service desk in the initial stages of the MDM Service.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

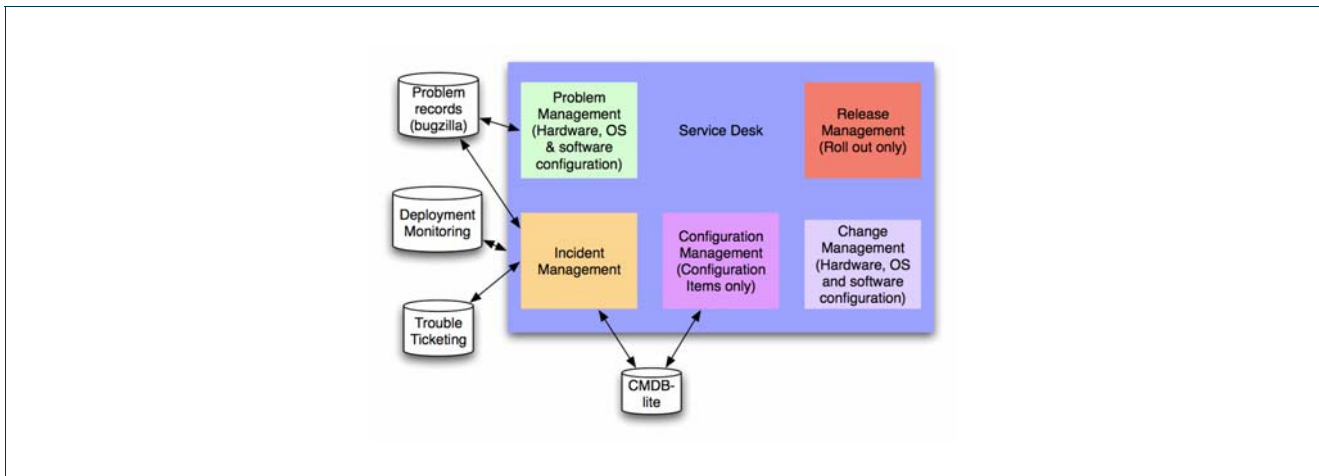


Figure 3.2: Service desk and its roles

The Service desk team for the MDM service will have at least two dedicated members of the DANTE staff. The Service desk will be available by telephone and email. During the initial stages, the Service desk is planned to operate between the hours of 08:30 to 17:00 UK time (09:30 to 18:00 Central European time).

3.1.2 Incident Management

The incident management process starts with the detection, registration and classification of incidents. The main objective is the resolution of these incidents, so that it can handle and restore any disruptions, or potential disruptions, to the service and thus ensure that the MDM service provides a high level of quality. Any disruption to the expected operation of the supported IT infrastructure (software and hardware) or any reductions in its quality get registered as incidents.

3.1.2.1 Incident recording and Classification

The Service desk plays a key role in detecting incidents from users' calls and also in proactively detecting incidents using the Service desk tools. Once detected, the incidents are recorded and then classified. The classification process is based on the impact of an incident and the urgency with which an incident needs to be resolved. The Service desk will make use of its experience and a defined set of criteria (for example the number of users affected, the effect of the incident on the users' activities, and so on) in order to assess the impact and urgency. Such an assessment will result in them being able to classify the incident with the right priority level. This priority is a key factor in determining actions of other processes, such as problem management and change management, for the incident. Hence, it is important that the incidents be prioritised appropriately.

In the initial stages, the Service desk will use a Trouble Ticket System as the primary incident logging tool. When logging incidents, it is important to link the incidents to the relevant IT infrastructure. For example, if a software installation in the NREN location (for example, N1) is reported as not working, it is important to record

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

the incident with all the details. It is also important to link this incident to the related IT infrastructure, for example:

“This incident is related to software type s1 with version number v1, working on a hardware platform with configuration h1, located in NREN location N1.”

In order to construct such relations, detailed information about the items that form the IT Infrastructure has to be stored and managed beforehand. Such detailed information will be stored in a tool called the Configuration Management Database (CMDB). The Service desk, with its role in the configuration management process, will maintain the information in CMDB. The configuration management process is discussed in more detail in a later section.

The CMDB contains detailed information about the items (or Configuration Items, CIs) that is part of the MDM Service infrastructure. CIs could be hardware information, hardware type, software, software version, and so on. A database system with administration and query interfaces will serve as an initial CMDB. This initial CMDB (called CMDB-lite for the purpose of differentiating it as a cut down version of the full CMDB, which will have more functionality) will only contain information about the CIs and not store any incident related information. Techniques to establish relationships between the Trouble Ticket System, the CMDB-lite (the database system) and other tools are currently being investigated.

In future, the Trouble Ticket System will be merged with CMDB-lite so that the Service desk can easily log incidents as well as map them with the affected items of the IT infrastructure efficiently, using the same tool. The status of the incidents, their resolutions and work-arounds will be recorded in the CMDB as well. The CMDB and CMDB-lite are discussed in more detail in later sections.

Some incidents might not need any investigation or diagnosis. The Service desk is expected to resolve such incidents without much effort. For incidents that require investigation, the Service desk follows the incident management procedures discussed below. It is the responsibility of the Service desk to ensure that the progress on a particular incident is constantly checked (and registered), and also to maintain communications with the affected users.

3.1.2.2 *Known Errors and Work-arounds*

Reported incidents are resolved either as “known-errors” or as “corrections” using a Request For Change (RFC). When an incident is recorded and prioritised, the incident management process first looks for similar incidents from the past. If no matching records are found, the incident is tagged as an “unknown error”, and a problem record is raised with the problem management team with the help of the problem management tool. The incident records are then updated with a reference to the newly created problem record.

If a matching incident is found and has an unknown error tag, the incident information is updated. Incidents can also be tagged as “known error”. In such cases, the incidents will have links to problem records in the problem management tool, and these records will have work-arounds or corrections available to resolve the incidents. If the Service desk is confident that such a matched incident is the same as the new incident being reported, they

will apply the work-around or correction and verify that this resolves the incident. If it doesn't, they will undo any actions and treat the incident as an unknown error.

Work-arounds are solutions to incidents that are effective enough to prevent the incident reoccurring or transforming into a different type of incident. They are usually temporary/quick fixes. Work-arounds usually do not involve making changes to the IT Infrastructure. For example: if large volumes of logs are being created and filling up the hard-disks, this could be reported as an incident. A potential work-around could be to use some temporary scripts to regularly clean up the generated logs. However, the proper solution to this could require a change to be made to the software to limit the volume of generated logs.

The problem management team is responsible for providing work-arounds for unknown errors and thus converting them into known-errors. These work-arounds are linked to the problem records and are stored in the problem management tool (Bugzilla). The next section on problem management discusses the process and the tool in more detail.

It is important to note that in case work-arounds don't exist, the incident management by itself will not try to identify the root cause or provide work-arounds. Instead, it will seek the help of the problem management team.

Figure 3.3 illustrates the relationship between Incident management and other processes.

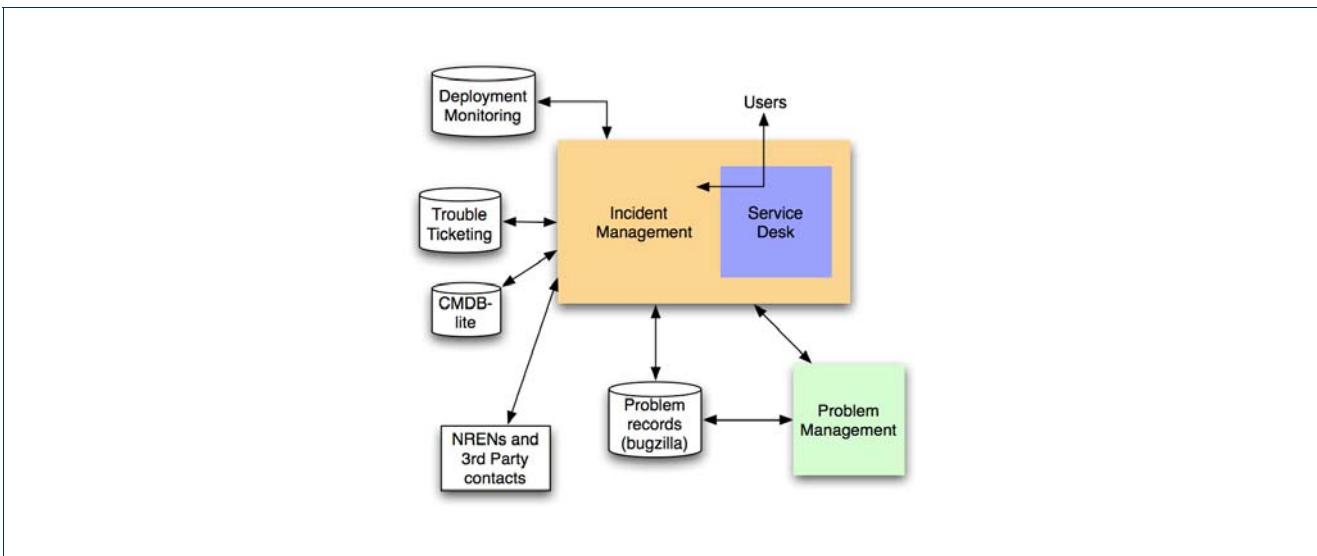


Figure 3.3: Illustration of communications between Incident Management and other entities

During the early stages of this service, incident management will make frequent use of problem management for any undocumented or unknown errors. In response, problem management will come up with a work-around and also record this with the help of the managed tools (Bugzilla). Eventually, as the incident records and work-around records get populated, the incident management teams will make use of these records and resolve the incidents quickly. At this stage, the number of problem reports being generated as a result of incident reports will reduce.

3.1.2.3 *Unknown Errors and Corrections*

Unknown errors get resolved either as work-arounds or as corrections. Corrections are a result of the problem management team being unable to provide a work-around, and hence requesting the change management process to provide a correction. This correction involves making changes to the IT infrastructure (such as new releases of software, updates, and so on). More information about this process is discussed in the sections on change management.

Making such changes usually requires a lot of planning in terms of cost analysis, impact, and so on. The time required to make such changes can be quite high. Therefore, the focus should be on trying to find work-arounds that can resolve the incident and restore normal operation as early as possible (but also to ensure that work-arounds are reliable and do not result in new/repeat incidents). However, it is very important for the MDM service to ensure that work-arounds get replaced with changes to the IT infrastructure so that incidents, which might get resolved quickly due to already available work-arounds, are avoided from occurring in the first place.

Hence, it is of utmost importance for all levels of incident management teams to remember that when incidents are reported, the primary goal of the incident management team is to resolve the incident and restore normal operation of the service within the shortest time possible.

3.1.2.4 *Incident Management Levels and Escalation*

Incident Management usually consists of multiple levels of incident management, where each level possesses a defined level of incident diagnosis skills. All these levels are lead by an Incident Manager.

Higher levels will have a more detailed view of the IT system, which can be used to diagnose and resolve complicated incidents or incidents that require an in-depth knowledge (for example: software development teams). For any incident, even if higher levels of incident management get involved and the incident is assigned to such teams, the first level team (the Service desk) will always retain ownership of the incident.

For the incident management of the MDM Service, at least initially, the Service desk will be the only level of incident management. This is because the intention is to start with a simple incident management process with clear procedures, which can then be reviewed and enhanced, based on performance and any enhancement requirements. The Service desk will have some basic system administration skills, which, along with documentation and support material, are sufficient to provide incident management for MDM Service.

One of the Service desk personnel will be assigned as incident manager. The incident management team will have contact details and contract obligations for hardware providers, and within the NREN organization. This is to help them in incident resolution requiring effort from external parties.

Escalation procedures will be defined in order to help the Service desk in the quick resolution of incidents. Hierarchical escalation procedures involve calling upon management (usually line management), to speed up resolution of incidents when other teams and external parties are involved. Such escalation procedures are currently being defined.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.1.3 Problem Management

The primary objective of problem management is to identify the root cause of unknown errors and to either provide work-arounds or to propose changes (using RFCs) to restore normal operation.

The Service desk and the development teams will constitute the problem management team for the MDM Service. The Service desk will investigate hardware and Operating Systems related problems, while the development team members will work on problems related to software products.

Even though the problem management team will have members who are also part of incident management team, it is important for the members to be aware of the procedures that need to be followed when they are playing these roles. The problem management team will be co-ordinated by a problem manager whose responsibilities are:

- Proper prioritisation of problem records.
- Assigning problem records to problem management team members for diagnosis and recovery.
- Following up on the progress of problem diagnosis and recovery.
- Ensuring that the problem records are kept up-to-date
- Escalating problem recovery process with other team managers, third-party providers, NREN contacts and project management.

During the initial stages of MDM Service, the problem manager will also play the role of the change manager. The responsibilities of the change manager are discussed in the section on the Change Management process. Figure 3.4 illustrates the communication between problem management and other teams. It also shows the involvement of Service desk and Development teams in the problem management process.

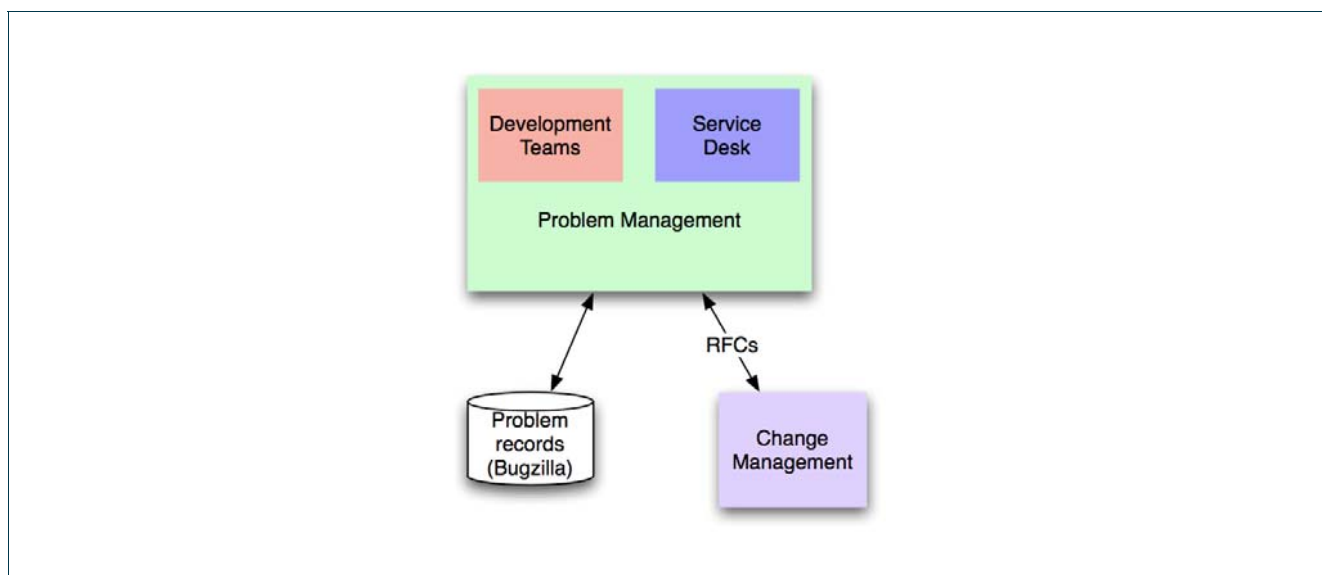


Figure 3.4: Illustration of communications between problem management and other teams

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.1.3.1 Problem Reports and Diagnosis

Problems are reported by the Incident Management Process or proactively by the Problem Management process. Other processes, such as the Release Management process, can also report problems to the problem management team. However, it is most likely that the incident management process will raise the majority of the problem reports.

As discussed in the previous section on incident management, the incident management team creates a problem report if it is unable to find matching incident records for a reported incident. Such problem reports are tagged as unknown errors. All problem reports will start with a priority value as requested by the reporting process/team depending on the impact of the problem. The problem management team, after analysis of the problem record, will reassign these priorities depending on other problems reported and resource availability.

Problem records will contain detailed information about the problem (including symptoms) along with information about the impact, the related IT infrastructure and the users. All problems should ideally be logged into the CMDB along with incident logs and Configuration Items. Relationships between all these entities should be established.

For example: An incident report should be linked to all related Configuration Items, such as software type and version, hardware platform configuration and affected users. If a problem record is raised as a result of an incident, the problem record will be linked to all the incidents that have been reported as well as the related Configuration Items and affected users. Such detailed information will help in the thorough investigation of the underlying cause of the problem.

However, such an integrated CMDB tool for MDM Service requires extensive tailoring to meet the needs of the service, and hence will not be implemented initially. In the short term, the GN2 JRA1 activity has been using Bugzilla to record reported problems. This tool will remain in use with some modifications. These modifications include establishing relationships between recorded problems and any incidents recorded in the Trouble Ticket System that triggered the problem report. The incident management process will be in charge of maintaining the relationship between incidents and problem records raised as a result of these incidents. Relationship between problem reports and related IT infrastructure will also be established.

3.1.3.2 Work-arounds and Request For Changes (RFCs)

When a problem record is reported, its default status is unknown error. The problem record will contain a lot of information, which will help the problem management team to diagnose the problem and discover its root cause. If required, the diagnostic process could involve simulating the problem in a test environment in order to help the problem management team establish the root cause.

Once the cause is established, the problem management team will either try to provide a work-around or propose a change, depending on the priority and impact of the problem. As described previously, work-arounds are solutions effective enough to prevent the incident reoccurring or escalating. They are usually temporary/quick fixes. Work-arounds do not usually involve making changes to the IT Infrastructure. Providing work-arounds will have a higher priority than making a change if the impact of the problem is high (for example,

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

a support piece of software is unusable by the users or a hardware component has failed resulting in hardware and software crash). Once work-arounds are available for unknown errors, the error gets re-classified as a known error.

If the problem management team cannot provide a work-around, or if the impact of the problem is very low and hence a work-around is not the ideal solution, the problem management team will propose a change to the IT infrastructure to resolve the incident/unknown error. Changes are proposed to the change management process for approval and for the actual change process to happen. The problem management team creates such proposals using a pre-defined RFC template. This will help in making sure that the information required from the Problem management team in order to decide on a change is available in the RFC. The MDM Service will make use of templates and sample documents for such RFCs.

If the problem management team cannot establish the root cause of a problem or cannot simulate the problem in a test environment, it is very unlikely that it will be able to suggest a work-around or propose an RFC. In such cases, the impact of the problem on the service and the number of users affected will be re-analysed to decide whether to carry out further diagnosis or to wait until similar problems are reported and any new information is available to help the diagnosis. Such decisions will be made in consultation with the managers of other processes and, if necessary, project management will be involved as well. In circumstances where the impact of the problem is very high and a remedy is critical, problem management will work with change management and project management to propose changes that are likely to be expensive and resource consuming.

3.1.3.3 Escalation

In order to ensure that the problem management team provides a quick and effective recovery for reported problems, escalation procedures will be defined. The problem manager will be responsible for all escalated problem records. Examples of situations that could require escalation are:

- For problems with high impact, the problem management team is unable to diagnose the problem or simulate the problem in a test environment.
- Problem management team can only suggest an RFC which is very expensive in terms of time and effort required.
- Delays in recovery due to involvement of third-party providers.

3.1.3.4 Proactive Problem Management

The scope of problem management is not limited to reactive diagnosis, but also includes the proactive identification of incidents that might arise in the future. The problem management team will proactively look into incident records to identify patterns that indicate potential underlying problems in the IT infrastructure. After further analysis, the problem management team will raise a problem record by itself and start to diagnose the problem. After diagnosis, the team will try to propose changes or provide work-arounds, so that either the incidents are avoided or expected incidents can be resolved quickly. If a change is needed, IT infrastructure will be improved in order to avoid such incidents.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.1.4 Change Management

The objective of change management is to ensure that all changes being proposed for the IT infrastructure go through a process of review, approval, implementation, and follow-up. The review phase involves gathering all the information available related to the change, such as reason for change, change priority, the IT infrastructure affected, details of change and the person/team requesting the change. It also involves calculating the costs for the change in terms of the required manpower and time, and also the impact on the IT infrastructure once the change has been made. The approval phase takes a broad look at the factors available and decides if the change can be authorised. This phase is highly influenced by the priority of the change. Once authorised, the change is implemented, tested and released. A follow-up is done to ensure that the change has produced the effect intended by the RFC.

The change management team will consist of a change manager leading a team of change builders. The responsibilities of the change manager are to:

- Gather information about the requested change (expected cost, priority, impact, and so on).
- Depending on the gathered information, consult with the project managers (also called the Change Advisory Board). The change manager can authorize minor changes without project managers' approval.
- Either approve or reject the RFC.
- Assign change builders to implement the change.
- Follow-up on the change implemented.
- Record all decisions and changes.

For the MDM service, the change management team will be made up of developers from various development teams as well as the Service desk personnel. Service desk personnel will be involved in all hardware related change implementation, while the development teams will be involved in both hardware and software product related changes.

3.1.4.1 Request For Change (RFCs)

RFCs provide a formal way to request a change to the supported IT infrastructure (hardware and software). The creation and logging of these RFCs is an important step in ensuring that the processes defined for change management are followed. RFCs can be issued not only by the problem management team, but also by other teams (such as development and release management).

For example, the development team might create new products that are expected to work with the existing IT systems. In such cases, the change management team's involvement is necessary in order to make sure that the introduction of such new products does not cause unexpected incidents and degradation of service. The release team could also propose changes to the IT infrastructure in order to help them in the release and delivery of software.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

At the beginning, the change management team will not make use of any dedicated tools to record and analyse RFCs. Templates and sample documents will be provided to help other processes write up RFCs. Once received, all RFCs will be registered by the change management process in a simple logging system that is currently being investigated. All RFCs received will go through an approval phase, and if approved will be implemented and tested. If RFCs are not approved, the change manager will log information about the reasons for the rejection.

3.1.4.2 Change implementation and follow-up

After a change has been authorized, the change manager will appoint a change implementer. This change implementer will either implement the changes by himself/herself or lead a team to carry out the changes. For all major changes, a “back-out” plan will be prepared by the change manager to ensure recovery if the changes are not successful. Once the changes are made, they will be tested by an independent testing team and then rolled out. This testing and roll-out is done with the help of the Release management team. If the changes were prompted by incidents, then after the changes are rolled out and applied to the IT infrastructure, the change manager will follow-up with the incident management team to see if the results are satisfactory and if the incidents are resolved. If not, a rollback will be required and the change process will need to be started again. If any changes are made to the IT infrastructure, the change manager will notify the creator of the RFC that initiated the change.

3.1.5 Release Management

The objectives of the release management team are:

- Preparation of products (new products, upgrades, patches) for release.
- Testing the products.
- Documentation and verification of other relevant documents.
- Roll-out of products.
- Maintenance of a Software Library for released products (DSL – Definitive Software Library) as well as dependency products.
- Maintenance of a Hardware Inventory.
- Collaborate with Configuration Management and Service desk on updating information about Configuration Items in CMDB-lite and Bugzilla.

The release management team will need to interact frequently with the change management team, the Service desk and the configuration management team. The release management team will be led by a release manager who will be responsible for the co-ordination of all these tasks listed above. The existing Release Management process, which was setup for the Release Management of GN2 JRA1 activity, has addressed most of the objectives listed above. The Service desk will be involved in the release management team process, and their tasks will be to assist the release management in rolling-out products and to setup and maintain a hardware inventory.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.1.6 Configuration Management

The configuration management team's main objective is to ensure that the data present in the CMDB is accurate and complete. The configuration management team will also be in-charge of generating reports on the contents of the CMDB. The team will also analyse the CMDB to detect anomalies in the stored information and get such anomalies corrected by contacting other processes and members.

During the initial phase of the MDM service, the Service desk personnel will be in-charge of Configuration management processes. However, their management will only be restricted to the CMDB-lite and the Trouble Ticket System. They will also be responsible for maintaining any data relationships between the Trouble Ticket System, Bugzilla and the CMDB-lite. However, Bugzilla contents will be updated by the problem management team and the Definitive Software Library, which is already in place, will be maintained by the Release Management team.

The Service desk will be expected to generate reports on the contents of CMDB-lite, as well as reports involving various statistics on incident management data. The problem management team will generate reports on problems and the change management team will generate reports on changes made to the software.

3.2 The Tools

This section provides a summary of all the tools that have been discussed so far. It also lists the processes that will be involved in using and maintaining these tools.

3.2.1 CMDB and CMDB-lite

Configuration Management DataBase or CMDB is a database used to maintain comprehensive information about the IT infrastructure. Most importantly, it maintains information about the following:

- The various 'Configuration Items' or CIs, which are part of the IT infrastructure.
- Incident related information.
- Problem records, work-arounds and information about RFCs raised as a result.
- All RFCs and their status, Change logs.
- Definitive Software Library.
- Relationships between all these entities, which includes relationship between incidents, work-arounds, problem reports, changes and the affected Configuration Items.

Detailed information of this kind helps all the teams in the analysis of the IT infrastructure required for their processes, and it also helps in generating reports. For the Configuration Items, the CMDB requires that all useful and applicable relationships between such items be maintained as well. Examples of configuration items are

- Software - Software or software component name and version.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

- Hardware - hardware name, hardware type.
- Operating System details – OS type, version.
- Deployment details - deployment location, important dates, person(s) in charge of deployments, and so on.

An example of a relationship between various CIs is: Software with id: s1 is installed on workstation with id: ws1 running Operating System with id: os1. This workstation – ws1 is deployed in location: loc1 and person in-charge has id person-1.

3.2.1.1 CMDB-lite

Designing and setting up a CMDB requires a lot of effort as it has to be tailored specifically to the requirements of the MDM service. Hence, the setup time and cost factors play an important role in deciding the capabilities and the depth of the information to be stored and managed in the CMDB. During the initial stages, the capabilities of the CMDB will be distributed among various tools, which are listed below. Information about Configuration Items, which forms the core of the CMDB, will be stored in a lightweight version called CMDB-lite (in order to differentiate its capabilities from the capabilities of the comprehensive CMDB system).

The CMDB-lite is a simple version of the CMDB that will contain basic Configuration Items which are critical to MDM service but are easy to maintain. It will focus on key Configuration Items and key relationships between these configuration items. The existing GÉANT2 Operations database will be used for this purpose. CMDB-lite will not contain any information about incidents, problems and RFCs. Correlation between the information in the CMDB-lite and in other tools will be achieved through the other tools and not CMDB-lite. For example, when incidents are logged in a Trouble Ticket System, the incident records will contain a reference to the data stored in the CMDB-lite.

Transition from CMDB-lite to CMDB will start during Year 4 of this activity, and will depend on the feedback received from various teams. Transition will be achieved by extending the operations database so that historical information is preserved and any effort required to migrate existing information to the new system is minimised.

3.2.1.2 Processes that will use the CMDB-lite

The following processes will interact with the CMDB-lite:

- Incident Management process: Linking incidents to configuration items, linking problem records to incidents and configuration items.
- Change Management Process: During analysis of an RFC, understands the impact of a change and also applying a change to all related Configuration Items.
- Release Management Process: Updating information about releases and updates with the help of the configuration management process (both hardware and software).
- Configuration Management process: Updating information about, verifying the validity of the information stored in the CMDB-lite.

3.2.1.3 CMDB-lite Maintenance

The CMDB-lite (and CMDB) will be maintained by the Configuration Management process. Whenever any process wants to update the CMDB-lite, the configuration management process will be involved and made aware of the changes.

3.2.2 Trouble Ticket System

A Trouble Ticket System will be the initial solution for incident management. Existing Trouble Ticket System solutions are being investigated for this purpose. Every time a ticket is raised/incident is logged, the information logged in the ticket is expected to include a link to the appropriate configuration item(s) present in the CMDB-lite. Whenever the status of an incident is changed or a resolution is applied, the information about resolutions, the links to work-arounds and problem records, will be added to the incident record.

The Trouble Ticket System is planned to be integrated with the CMDB system during Year 4 of this activity. Such integration will require the migration of historical information (existing trouble tickets) into the CMDB system.

The Incident Management system and the configuration management process are the only processes that will use the Trouble Ticket System. The incident management process will maintain the Trouble Ticket System.

3.2.3 Problem management tool - Bugzilla

The Bugzilla tool that serves as a problem management tool is currently installed and is in widespread use by the GN2 JRA1 activity. This Bugzilla will be used as the primary problem management tool for the MDM Service. Whenever a problem needs to be reported, the incident management team will report the problem in Bugzilla and update their incident record with the appropriate problem record information (automatically generated by the tool). The Problem management team will, however, be in charge of managing this tool and keeping it up-to-date. Any work-arounds will be linked to problem records by the problem management team. The incident management team will therefore be able to search through problem records and obtain applicable work-arounds.

The possibility of extending Bugzilla to help in change management process is currently being investigated. Although templates for RFCs will be provided, RFCs need to be recorded and change records need to be maintained.

3.2.4 Deployment monitoring system

A deployment monitoring tool is already implemented. This tool constantly queries the configured deployments to check their status. If any deployments are unavailable, the tool raises an automated email alert and sends

such alerts to contact personnel for these deployments. The tool also records the status of the configured deployments, and generates graphs showing the historical status of each and every configured deployment. This information will be used by the incident management in reporting the status of software deployments across the NREN community.

This existing tool will be of immense help to the Service desk in proactively detecting incidents before the users report them and also in generating reports on the status of deployments. It will be enhanced further in its capabilities to assist the Service desk in gathering more information about the incidents. The Service desk and the contact person for the deployment (NREN contact person) on the list of people notified automatically when the status of a deployment changes.

3.3 Use cases

This section illustrates how common use cases are handled by the above described ISS Structure. Each flow chart is more detailed for the particular area that the use case focuses on.

3.3.1 Use case – 1: Incidents resulting in known-errors

Figure 3.5 illustrates the process of detecting incidents requests coming from the users. It focuses on how incidents get resolved as known errors.

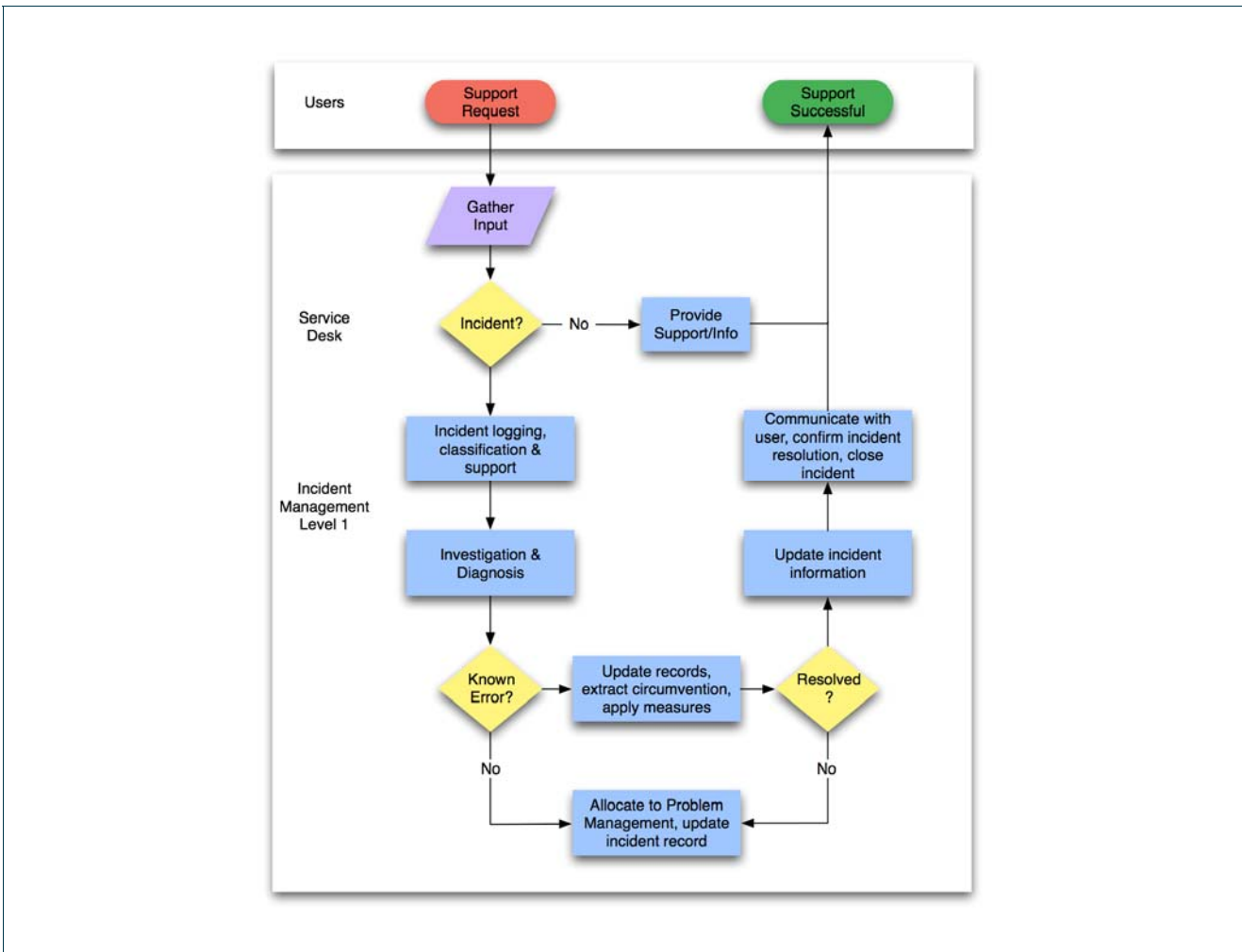


Figure 3.5: Flow chart illustrating use case 1- Incidents which are known errors

The Service desk, which is involved in incident management, will gather and analyse input from the user asking for support requests. If incidents are detected, the Service desk begins the incident management process. If not, the Service desk provides the necessary support or information required.

If incidents are detected, an incident record is created and detailed information about the incidents is logged. Depending on the impact and urgency of the incident, an appropriate level of classification is assigned. Depending on the classification, the incident is either investigated immediately or at a later time. Initial investigation involves finding out if the incident has occurred before, and if there are any known errors and work-arounds available. If a work-around is found, it is applied to see if the incident is resolved. If it is resolved, the incident is closed. Otherwise, a problem record is raised with the problem management team. If a work-around is not available, the problem management team is approached in order to find a work-around so that the incident can be resolved.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.3.2 Use case – 2: Incidents, unknown-errors and creation of work-arounds

Figure 3.6 illustrates how the incident management team will interact with the problem management team in case of an incident for which no known-error and work-around information is available.

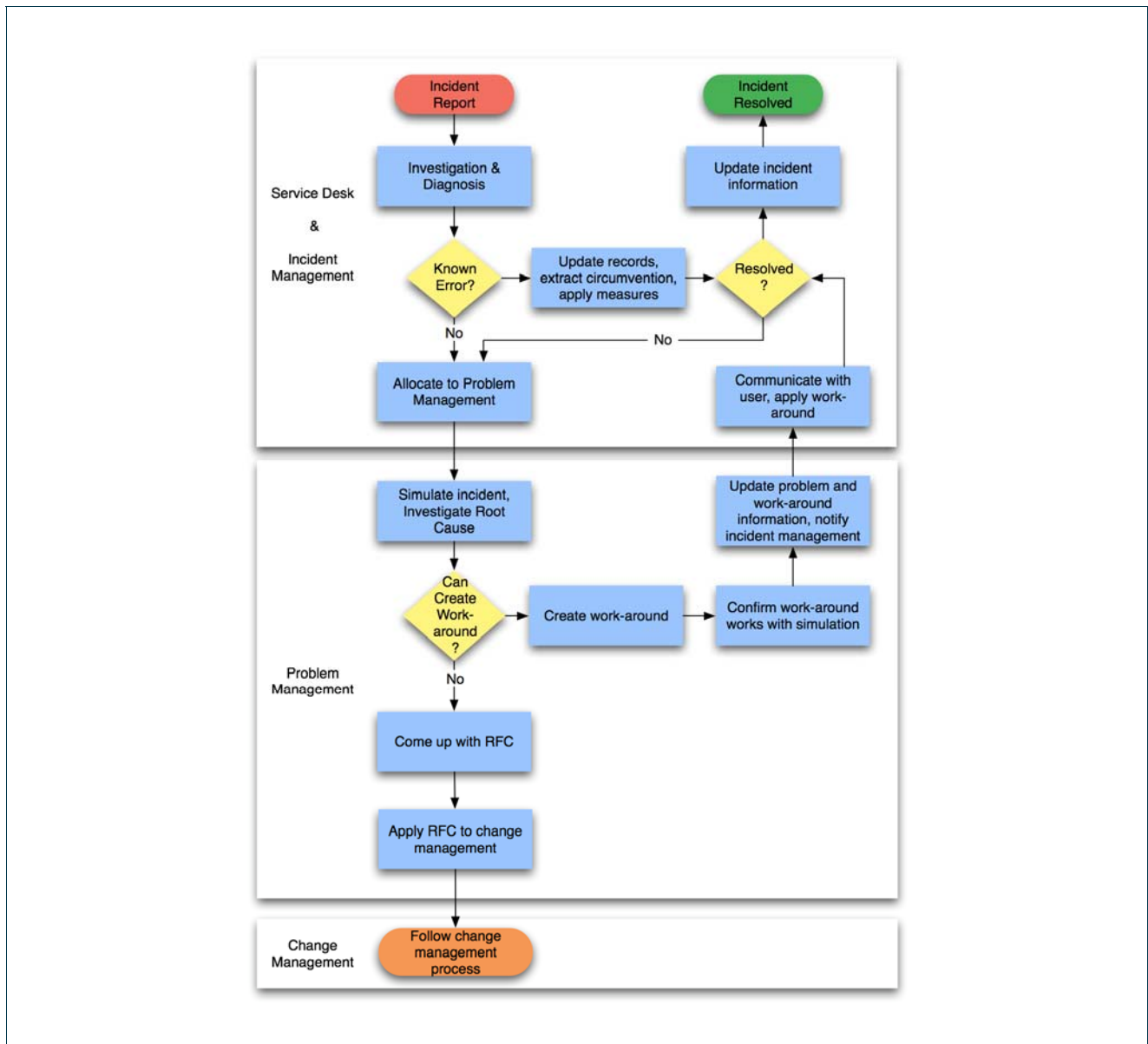


Figure 3.6: Incident resulting in RFC being generated by the problem management team

The problem management team tries to simulate incidents and investigate the root cause of such incidents. If work-arounds are feasible, it will try to come up with a work-around. If not, it will propose a change to the change management team using RFCs. The change management team will follow change management processes (not described here)

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.3.3 Use case – 3: Incidents, unknown-errors and resolution using RFC

Figure 3.7 illustrates a use case where the change management team follows procedures in order to evaluate a change and get the change built.

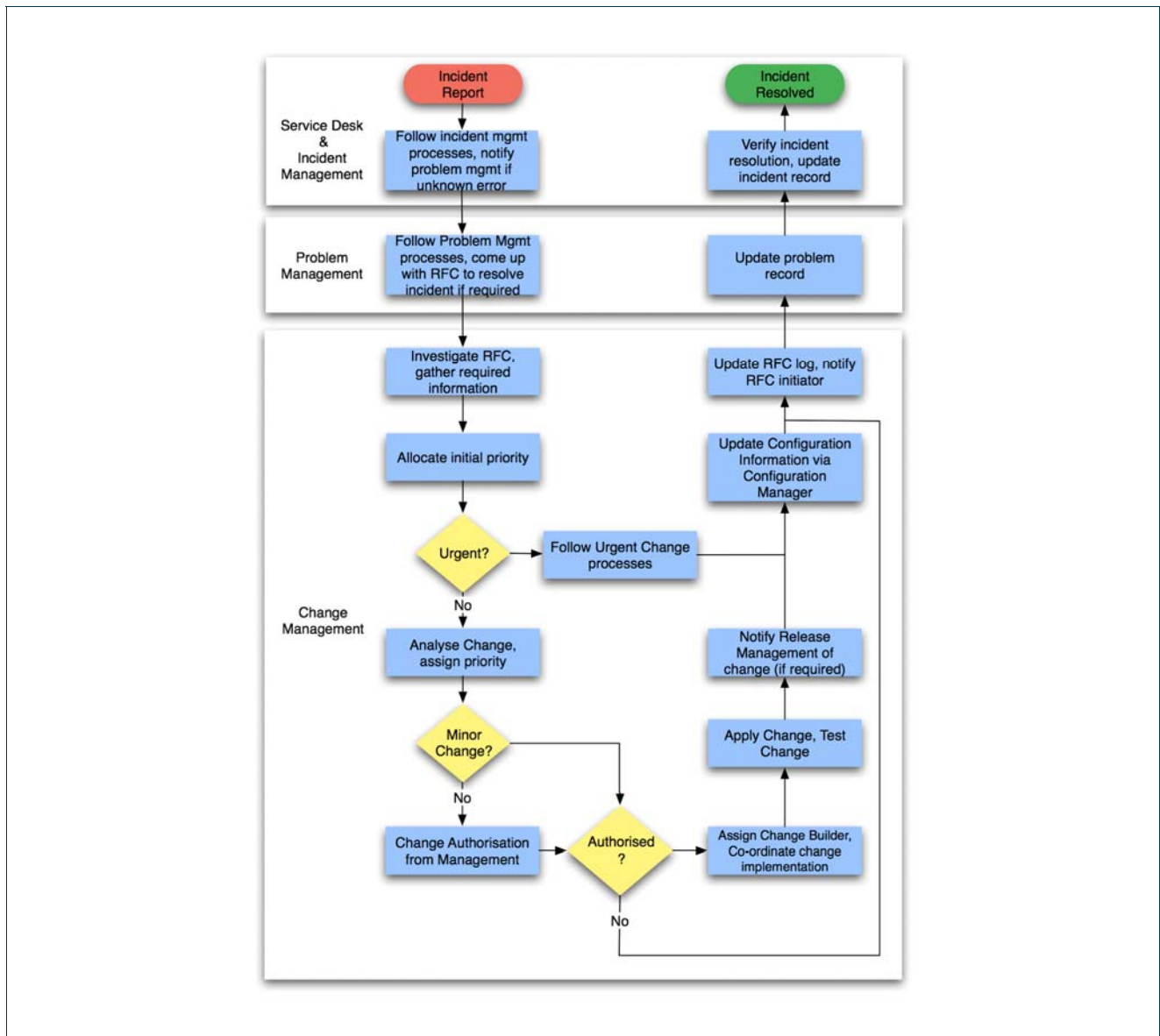


Figure 3.7: Flow chart illustrating change management procedures being followed

Upon receiving an RFC, the change management team tries to investigate the urgency of the change. If urgent, an expedited change process is followed (not described above). This expedited change process is similar to the change process of an RFC with normal priority but with shorter timeframes, quicker decisions and some aspects of the process not followed in order to reduce the turn-around time.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

The change management process goes through a change analysis and authorisation process. After that, the change is made and communicated to other involved teams as well as the user.

3.3.4 Use case – 4: Proactive incident and problem detection

Figure 3.8 illustrates how various processes can help in proactive incident and problem detection. Once detected, the processes followed for resolving such incidents are similar to any other incident. Prioritisation of such incidents could end up being high (to reduce its impact) but this depends on the impact and urgency factors.

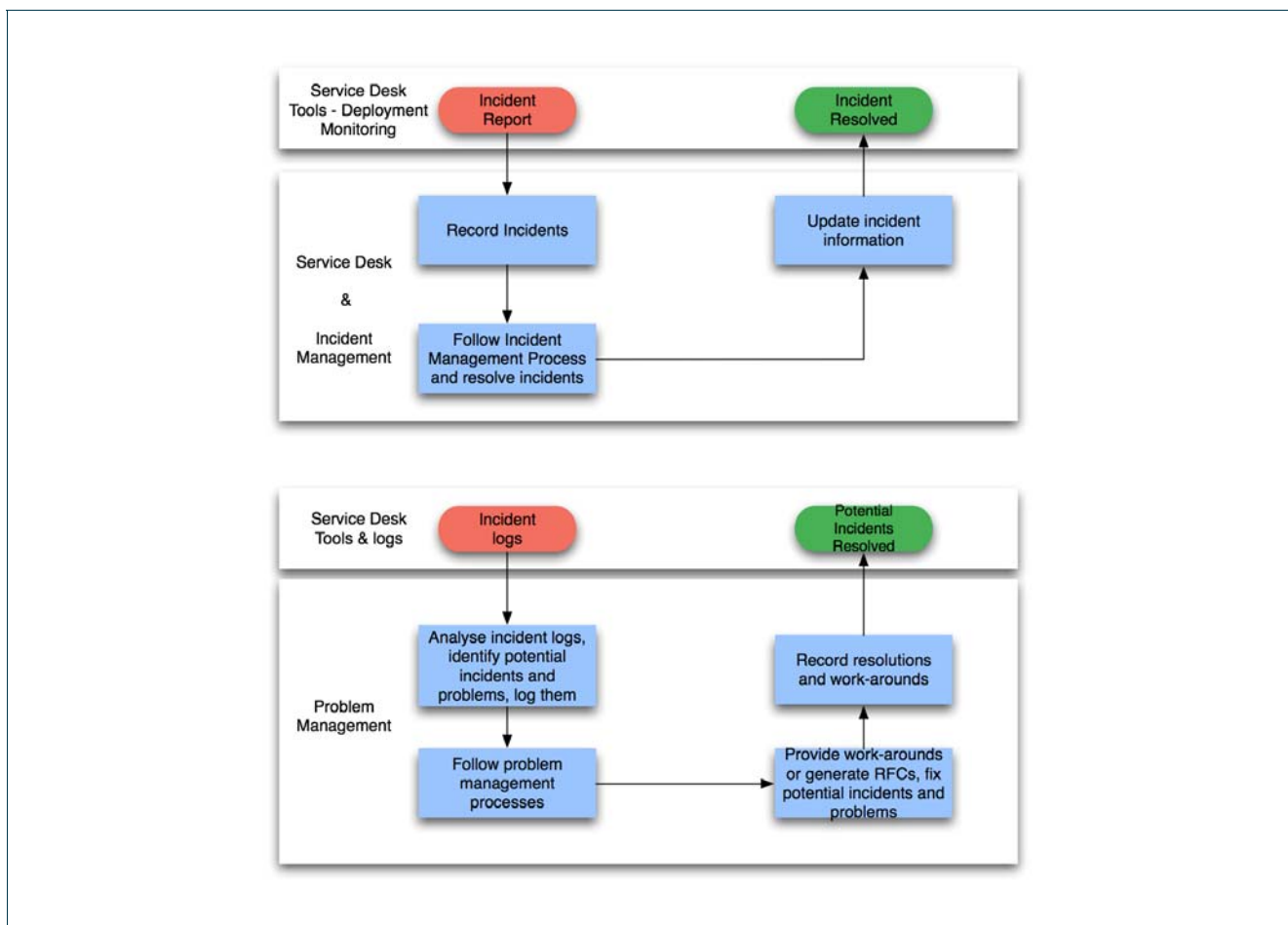


Figure 3.8: Illustration of proactive incident and problem detection

In the top half of the figure above, existing deployment monitoring tools aid the Service desk in proactive incident detection (find out the status of deployments before the user experiences it and reports to the Service desk). In the bottom half, the problem management team is seen analysing the incident reports and trying to find out if there is an inherent problem which is or which might generate issues.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

3.3.5 Use case – 5: Introduction of a new product

Figure 3.9 illustrates the process for adding a new product into the IT service catalogue. Change management is the most important part of this process.

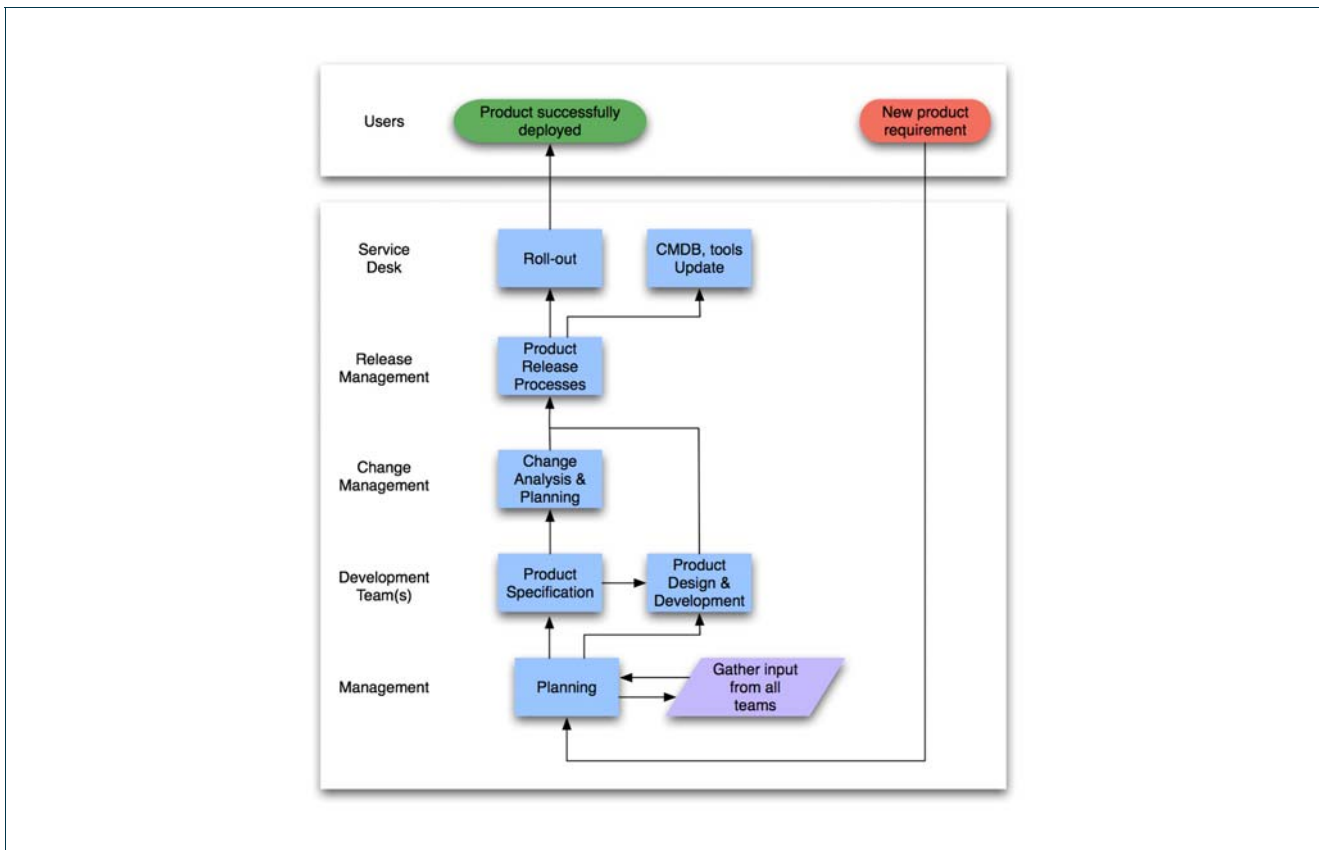


Figure 3.9: Flow chart illustrating Introduction of a new product

The process starts with a requirement for a new product. Project management captures the requirements from the users either from the Service desk or a formal requirement capture process. The management then consults with the teams to plan resources and timelines for the introduction of the new products. Product specifications are then written up by the development teams. The change management team provides invaluable information during this specification phase to ensure that the product can be supported when it goes into service. Interoperability factors with other IT systems (if required) are expected to be one of the major factors. This phase could go through a number of iterations of planning and design.

After the specifications are agreed, the product is designed and developed. During this phase, change management will plan the implementation of any changes required to the IT infrastructure. Once all this is done, the product will go to the release management team for quality control. When accepted, it is rolled out by the release management team.

Project:	GN2
Deliverable Number:	DS3.15.1
Date of Issue:	21/05/07
EC Contract No.:	511082
Document Code:	GN2-07-118v2

Service desk involvement is expected in roll-out and communication with users. Service desk is also expected to update the CMDB with the changes. When the product is deployed successfully, all teams are notified and the product will have entered into an operational support phase.

3.4 Service Portfolios

Service Portfolios define what support a user can expect to receive. Successful operation of the software supported by MDM Service depends upon the correct installation, configuration and operation of:

- Hardware resources
- Operating Systems
- MDM Software

The Service Portfolios initially being offered are described below. This list will be improved based on feedback and experiences.

MDM Service supports a number of software products for NRENs to choose from. Most of these products can be coupled with any of the service portfolios available. However, for certain software products, the choice of portfolio may be limited. Such choices and limitations will be explained in the MDM Service Catalogue.

3.4.1 Managed Service Support (Hardware and Software Support)

This portfolio provides support for software, Operating System and hardware. This is achieved by procuring hardware, installing and configuring the Operating System, installing and configuring the necessary monitoring software, and shipping the whole package to the customer. Once this is done, the maintenance of the hardware and software installation is carried out by support teams. The intention here is to:

- Reduce the initial effort required on the NREN side for installation and configuration of the software on the hardware.
- Reduce day-to-day effort required on the NREN side for hardware and software maintenance.
- Improve support efficiency due to the hardware being known, rather than having to investigate if an unknown piece of hardware is causing problems.
- Bring about similarity among hardware and Operating Systems used for software deployments thus improving service reliability and providing faster support.

The NRENs interested in taking up this option will have well defined methods of interaction with the hardware and software installations, and this will ensure that the NRENs have control over both elements. Due to the nature of the software developed by the GN2 JRA1 activity, the involvement of the NRENs during the installation and maintenance is also expected. Some software produced by GN2 JRA1 activity (for example: One way delay measurement systems) makes it a requirement that only the managed service option be made available to NRENs interested in this software.

Support for any hardware procured and used for providing this portfolio will be dependent on contracts with third-party hardware vendors and vendors of dependency software, such as Operating Systems. Such support constraints will be made known to the NRENs in advance.

3.4.2 Software-only Support (Support restricted to a set of Applications)

In this portfolio, NRENs will procure the hardware and deploy the specified set of software. The Service desk will provide assistance in any issues arising during the installation, configuration and day-to-day working of the software (usually restricted to software supplied by the GN2 JRA1 activity).

All Hardware and Operating System related issues will be dealt with solely by the NRENs even though the type of hardware and list of software dependencies required are specified by the project itself.

Due to the element of hardware and Operating System problems, any unavailability of service due to such problems will not be considered as downtime for the software service being offered.

4 NREN Participation

4.1 Incident Management and Service desk

Incident Management process for the MDM Service will only have one level of incident management during the early stages and this will be provided by the Service desk. DANTE will have members of staff dedicated to the Service desk. The incident management process will communicate with the various NREN contact persons and also third-party providers whenever required during the incident management process.

4.1.1 Problem Management

The following NRENs will be involved in problem management:

- ARNES
- BELNET/University of Gent
- CARNet
- CESNET
- DFN
- ISTF-ACAD (BREN)
- NORDUnet
- PSNC
- RedIRIS
- SURFnet

4.1.2 Release Management

The following NRENs will have a major involvement in Release management:

- FCCN
- CyNet
- GRNET

Apart from the above list, other NRENs will be involved for short periods (for example: Usability testing).

4.1.3 Change Management

Along with DANTE, the following NRENs will be involved in change management and change building:

- ARNES
- BELNET/University of Gent
- CARNet
- CESNET
- DFN
- ISTF-ACAD (BREN)
- NORDUnet
- PSNC
- RedIRIS
- SURFnet

4.1.4 Other

All NRENs participating in the GN2 JRA1 activity will be involved in many other areas directly or indirectly related to ISS, such as management, documentation, training and dissemination.

4.2 Current Status

The implementation of various processes listed above began towards the beginning of this year. Although there was an existing release management process used by GN2 JRA1 and other partners for the perfSONAR project, this process has been redeveloped, taking into account the requirements of transition to service. A new version of the perfSONAR bundle has been produced using the improved release management processes. This document details the objectives and plans that are currently being pursued.

Procurement of hardware required to support the Managed Service has started and deployment of software will begin soon. Some of the tools listed above, such as the Trouble Ticket System, are being evaluated. Other tools, such as CMDB-lite (DANTE Operations Database) and Bugzilla, are being upgraded to meet the requirements of the MDM Service.

5 Conclusions

A large part of the planned support structure is currently being implemented. This support structure will be enhanced based on the feedback from this implementation.

A key area where work will be carried out in future is the service delivery aspect of the MDM service. Service delivery deals with long term planning and improvement of the MDM Service provision. It defines many other processes, such as Service Level Management, Availability Management, Capacity management, Financial Management and IT Service continuity management.

As part of Service Delivery, Service Level Agreements (SLAs) will be drawn up based on the experience gained during the pilot and prototype phases. SLAs provide detailed information about the level of support that the users can expect from the service. The key objectives of all the processes in Service Delivery are to verify SLA adherence, continuously gather requirements, and on the whole improve the MDM service provisioning.

The GÉANT2 project will provide more services using products from activities such as the GÉANT2 Identity Provider (GIdP), the Advanced Multi-Domain Provisioning Systems (AMPS) and the GN2 JRA4 E2EMon (E2EMon). The processes discussed in this document for the MDM Service will be reused for all new services.

6 References

[AMPS]	http://www.geant2.net/server/show/nav.1527
[BS15000]	http://www.bs15000.org.uk/
[BUGZILLA]	www.bugzilla.org , www.bugzilla.perfsonar.net
[E2EMon]	http://wiki.perfsonar.net/jra1-wiki/index.php/PerfSONAR_support_for_Lightpath_Monitoring-LHC_project
[GIdP]	http://www.geant2.net/upload/pdf/GN2-06-326v7-DS3-14-1_GEANT2_Identity_Provider-GIdP-Design.pdf
[ITIL]	ISBN: 0 11 33 0015 8
[itSMF]	ISBN: 0-9524706-1-6 www.itsmf.com
[OGC]	www.ogc.gov.uk
[PERT]	http://www.geant2.net/server/show/nav.1528
[SMOKEPING]	http://oss.oetiker.ch/smokeping/

7 Acronyms

CI	Configuration Item
CMDB	Configuration Management Database
CMDB-lite	Configuration Management Database – light weight
DSL	Digital Software Library
ISS	In Service Support
ITIL	IT Infrastructure Library
MDM	Multi-Domain Monitoring (Service)
NREN	National Education and Research Network
OGC	Office of Government Commerce
PERT	Performance Enhancement and Response Team
RFC	Request For Change
SLA	Service Level Agreement
SPOC	Single Point Of Contact