POL00394097

PinkRoccade

End to End Service Report

Service Management

Client: Post Office Ltd

Laura Sharpe, George Kincaid, Mick Conlon and Phil Marland

Company: PinkRoccade UK
Reference: POL/758R
Version: 1.0 (Final)
Date of publication: May 20, 2002

POL00394097

Document Control

Reference Number:	POL/758R
Document Title:	End to End Service Report
Client:	Post Office Ltd
Version Number:	1.0 (Final)
Date of Publication:	May 20, 2002
Author(s):	Laura Sharpe, George Kincaid, Mick Conlon and Phil Marland
Quality Assurance:	Chris Miles
Filename:	PO E2E SM Report V1.0 (Final)
Number of Pages:	94 Including preliminaries & appendices
Security Classification:	Commercially Confidential

Document History

Version Number	Recipient	Release Description	Release Date
0.2 Draft	Chris Miles	Draft for review	17/05/02
0.3 Draft	Laura Sharpe	QA feedback for review	17/05/02
1.0 Final	Post Office Ltd	Final report	20/05/02

Additional Documentation

Document Name	Recipient	Release Description	Release Date
-	-	-	-
-	-	-	-

POL00394097

Acknowledgements

PinkRoccade UK Consulting would like to acknowledge the high level of co-operation, openness and general communication shown by the interviewees within Post Office Limited throughout the compilation this report.

Management Summary

Post Office Limited (POL) will be launching the Network Banking Service in April 2003. In order to ensure the ongoing success of this service, POL has recognised the need for improved Service Management processes to support Network Banking from its launch date.

PinkRoccade UK Ltd were invited by POL to undertake a 6 week study to consider, assess and recommend an optimum Service Management framework to support the environment leading up to and post Network Banking. This 'ideal solution' will span the multi-vendor environment encompassing such features as:

- A Technical Service Desk (TSD), to form a single point of contact for the technical aspects of the Service Management framework.
- A more centralised approach to Service Management.
- Integration between existing tool sets
- The production of End-to-End management information across all Service Management disciplines.
- Definition of clearer roles and responsibilities

This report details the results of this work.

High Level Recommendations

The introduction of the Network Banking service will involve a period of significant change. The current Service Management processes within POL are not sufficiently mature to support this new service. Proven industry studies show that insufficient investment within the areas of Service Management at such times can lead to lost revenue through increased downtime of critical business services.

a) POL should invest in an End-to-End Service Improvement Programme (SIP) focusing on the People, Process and Technologies within the support environment. A project plan should be devised that embraces the recommendations within this report. This plan should be in the form of a properly constituted project, being managed using proven methodologies such as PRINCE2. The activities contained within this plan should be prioritised in the order most beneficial to POL.

POL00394097

b) The Service Management processes within POL are currently fragmented across the business. This contributes to the following factors: -

- Poor communication between teams.
- No overall (end-to-end) view of each process areas.
- Areas of responsibility and ownership are unclear.

To improve performance, a rationalisation exercise should be conducted that creates single teams responsible for the end-to-end Service Management processes under one Directorate.

c) Consideration should be given to the initiation of a work package to review the tool sets that support the Service Management processes. The objectives of this work package are to identify the options available to POL for establishing an integrated tool set across the business, or at least providing a level of Integration between the existing tools.

POL00394097

Indicative Costing

An indicative cost model has been produced by PinkRoccade to provide budgetary guidelines for the Service Improvement Programme. Each process area has been assessed and guidelines are provided for the Achievable, Desirable and Ultimate levels of improvement. These are summarised in the table below and can be seen in more detail in the costing section of this report:

	Current Process Maturity:		Achievable Solution (Cost)	Desired Solution (Cost)	Ultimate Solution (Cost)
Process:					
Incident	*Control*	PR	£49,500	£49,500	£99,000
		PO	£18,000	£18,000	£36,000
Problem	*Control*	PR	£49,500	£49,500	£99,000
		PO	£18,000	£18,000	£36,000
Change	*Awareness*	PR	£49,500	£49,500	£99,000
		PO	£36,000	£36,000	£54,000
Configuration	*Initiation*	PR	£72,000	£144,000	£216,000
		PO	£36,000	£72,000	£108,000
Release	*Control*	PR	£49,500	£49,500	£49,500
		PO	£18,000	£18,000	£18,000
SLM	*Control*	PR	£24,750	£24,750	£72,000
		PO	£18,000	£18,000	£36,000
Availability	*Absent*	PR	£72,000	£72,000	£120,000
		PO	£18,000	£18,000	£54,000
Capacity	*Absent*	PR	£49,500	£49,500	£82,500
		PO	£18,000	£18,000	£54,000
BCM	*Awareness+*	PR	£24,750	£24,750	£49,500
		PO	£18,000	£18,000	£36,000
Tools			£144,000	£216,000	£288,000
Project Costs:					
Managing Consultant			£121,500	£162,000	£243,000
Project Support			£58,500	£78,000	£117,000
Director			£9,000	£18,000	£27,000
	Total PR		£774,000	£987,000	£1,561,500
	Discounted		£530,600	£669,050	£1,042,475
	Total PO		£198,000	£234,000	£432,000
	Grand Total		**£728,600**	**£903,050**	**£1,474,475**

Notes: 1. POL costs are based on an estimate of £300 per day for internal resource (denoted as PO)
2. PinkRoccade costs are based on the rate card minus the agreed discount (denoted as PR)

POL00394097

Summary of Recommendations

The main recommendations, broken down by process, from this initial piece of work are as follows, for further details refer to the main body of this report.

Service Desk and Incident Management

- Implement a Technical Service Desk (TSD) to manage and take ownership of technical Incidents on behalf of POL. This desk will provide a skilled single point of contact for technical support requests.
- Formal relationships between Service Management processes needs to be established.

Configuration Management

- POL should outsource the technical Configuration Management (CM) function to the TSD, enabling them to concentrate on their core business, whilst still being provided with the necessary overall picture of the technical infrastructure that Network Banking presents. The outsourced CM function should manage a centralised CMDB using an appropriate support tool – to be agreed between TSD and POL.

- A Configuration Manager role should exist within the TSD. The role & responsibilities should be clearly defined between POL and the 3rd party supplying the TSD, with interfaces and expected reporting requirements agreed and understood by both parties.

Problem Management

- The role of Problem Management needs to be expanded to include future internal and external IT suppliers to POL.
- POL has undergone rapid changes over the last 12 months, it is essential that all documentation related to Problem Management be reviewed and updated with all the new name changes to reflect the current organisation.
- The Problem Incident Advisor (PIA) roles and the Process Efficiency (PE) analyst role should be combined to produce a single team that will effectively advise and mentor branches on operating procedures. It would also insure single ownership of improvements to be communicated to the branches. Clear lines of demarcation of roles and responsibilities need to be agreed between the Incident Management team and the Problem Management team, detailing how trend reporting and progression is accomplished.
- The Problem Management team does not have sight of a Forward Schedule of Change detailing all the planned changes to the IT Infrastructure of POL.

POL00394097

A review of how changes are communicated to Problem Management needs to take place.

- Working hours between Service Desks and Problem Management need to be synchronised, to ensure that disparity between operating times no longer exists. This will become more critical as the services offered to the branches increase with real time banking.

Change and Release Management

- Change Management should be centrally implemented and controlled within the Change and IS Directorate. However, Network Support should maintain final approval for releasing change into the Network Banking environment.
- A fully ITIL compliant Change Advisory Board (CAB) should be implemented
- Standard Key Performance Indicators should be defined and agreed to measure the quality of Change Management.
- Communication of changes is crucial. The TSD and NBSC should be made aware of all scheduled changes. The business should be aware of all non-operational changes where there is a risk of business impact.

Availability Management

- An Availability Manager role should be assigned to a suitable candidate within the Network Support area. This person will be responsible for the initial definition of the role and the creation of a formal Availability process within POL.
- The focus of Availability targets should be reviewed and consideration given to broadening the scope to include an end to end view of service availability.
- Appropriate tools should be investigated and implemented to aid the measurement of end to end component availability. This information will inform supplier meetings when discussing performance and reliability of supplied hardware and software. Where possible suppliers should supply accurate availability information at service reviews.

Capacity Management

- Consideration should be given to creating a process owner for the Capacity Management function. It is recommended that this role be allocated to a suitable candidate within the Operations Directorate. The resources currently allocated to this role for each platform should feed into this area. This would enable a picture of capacity utilisation, performance and requirmeents across all platforms to be established.
- A single Capacity Plan should be compiled within the framework of the above Capacity Management process as it relates to and is appropriate for POL. This plan should encompass all platforms and all connectivity within the Network Banking environment through to the end users. This would ensure that the issues were considered and adopted from the beginning. It would

POL00394097

also ensure that related Service Management processes are considered and interfaces built between them.
- Consideration should be given to the development of an End to End capacity model for the Network Banking environment.
- Steps should be taken to ensure that the POL Capacity Management function becomes involved in the lifecycle of projects to assess and advise on capacity requirements, to improve cost effectiveness, utilisation of resources and reduce the possibility of bottlenecks.

IT Service Continuity Management

- To further strengthen the process, more focus should be placed on understanding the technical continuity measures employed by each of the suppliers. This will require the development of additional technical skills within the team.
- The minimum levels of operation to be delivered in the event of a disaster should be communicated to the business. This will ensure that expectations of both the business and the branches are managed.
- Consideration should also be given to carrying out a simulated disaster to measure to assess the effectiveness of each supplier's continuity arrangements.
- POL should maintain the final approval of the invocation of supplier disaster recovery procedures.

Service Level Management

- SLM is a critical function and should continue to be totally owned and controlled by NS for the NB service. However the SLM function may employ the Fujitsu Services TSD to collect service data on its' behalf from the various suppliers.
- A comprehensive project plan (PRINCE2) for managing the SLM functions for NB needs to be instigated.
- Consideration should be given to appointing a NB service manager who will ensure End to End protection and assurance of the service on behalf of the customers.

POL00394097

Table of Contents

POL00394097

POL00394097

1 Introduction

The Network Support (NS) function within Post Office Limited (POL) is responsible for the support of Post Office branches throughout the UK, providing service to some 17,000 outlets and 38,000 counter terminals.

Broadly, this support service is divided as follows:

- Any support relating to the Horizons desktop system is provided by Fujitsu Services
- Any other support, for example relating to Post Office products, processes and service requests, is provided directly by NS

The introduction of Network Banking in April 2003 will significantly change the nature of the support services to be provided by NS. These changes will include:

- Potential increase in volume of calls
- The need for more immediate resolution of calls – since the service desk will be supporting real time transactions rather than batch
- The need to support a wider range of services, provided via multiple suppliers
- More complex calls
- Management of multiple supplier contracts and Service Level Agreements
- Complex Problem & Change Management activities potentially involving multiple suppliers
- Potential direct links with the customers on the street as well as PO branches

On 10 April 2002 Phil Marland, Chris Miles and Tony Price from PinkRoccade presented to Post Office Ltd senior management possible options for a new NS structure (specifically Service Desk) to focus any subsequent E2E Service Management solution work. A preferred option was selected by POL of a separate, possibly outsourced, Technical Service Desk. Since this selection it has been confirmed that it is expected to outsource the Technical Service Desk to Fujitsu Services.

PinkRoccade were asked to assist in the design of an End to End Service Management solution centred on the preferred option as detailed above, ensuring as far as possible that this solution factors in other NB or company-wide initiatives which are currently being managed.

Our approach encompassed the following key areas upon which this report is based:

- Recommendation of an End to End Service Management Solution to manage the Preferred Option (i.e. Fujitsu Services managed Technical Service Desk);
- Consideration of optimal Service Management Requirements for recommended solution;

POL00394097

- GAP analysis on existing NS Service Management process practice with recommendations to overcome any disparity;
- High level GAP analysis and consideration of tool requirement to support recommended End to End Service Management solution.

POL00394097

2 Ideal Service Management Solution

2.1 Functional Specification, Roles & Responsibilities

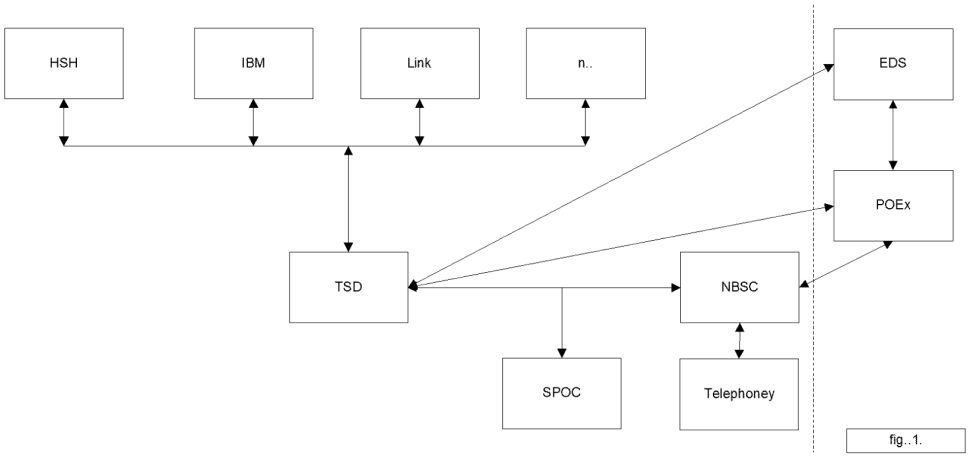
Functional Specification, Roles & Responsibilities of each Service Management Discipline

2.1.1 Service Desk & Incident Management

POL will retain the operational management of the business-related Service Desks for Network Banking Support Centre (NBSC) and the Post Office External Service Desk (POEx), utilising the existing customer supplier relationship between Network Support (NS) and Customer Management (CM).

POL is proposing to outsource the Technical Service Desk to a 3rd party with expertise in POL's existing technology and future technology requirements. The TSD will act as a skilled Service Desk and be responsible for incident resolution and incident management for the proposed new and existing technology for the Network Banking project.

The POEx Service Desk will be the first point of contact for the Public for incidents relating to the Card Account, any incidents that cannot be resolved by POEx will be passed to Electronic Data Systems (EDS). It is assumed that should there be any technical difficulties experienced by the Public whilst using their cards, they will escalate the incident to Post Office Staff at the counter where the incident has occurred. This will then be reported via the Interactive Voice Response (IVR) system as the Single Point of Contact (SPOC) utilised by the business to report technical incidents to the Technical Service Desk (TSD) for investigation or resolution.



The TSD will be the operational first point of contact for all IT incidents reported by the business. Where the TSD is unable to resolve the incidents, the incidents

POL00394097

will be passed to the 3rd party vendor contracted to supply and support the new or existing technology for Network Banking (NB). The individual vendors will be responsible for their own incident management processes, with TSD responsible for the overall management of an incident during its life cycle.

3rd party vendors will be responsible for progressing all incidents passed to them by the TSD. Where necessary 3rd party vendors may need to work together to investigate an incident managed by TSD. Where an incident occurs of significant impact or multiple incidents are identified, these incidents will become problems and escalated to and managed by the NS problem management team.

TSD will be responsible for the Management Reporting on Incident Management to NBSC, as they will be the central point of contact for technical issues with overall responsibility for the resolution of incidents.

2.1.1.1 Scope of process:

All customer calls to the Service Desks will result in an incident being raised.

The Service Desk will cover the following broad categories of incidents:

- IT systems (hardware/software) for Network Banking
- Telecommunications for Network Banking

2.1.1.2 Roles & Responsibilities (Post Office & Supplier):

The following suggested list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles required within the Service Desk function. Roles and responsibilities similar to these should also exist within each of the technical solution suppliers and the interfaces between the supplier and POL should be clearly defined:

Role	Responsibilities
NS (Post Office - Customer)	• Own the overall Incident Management framework process flow for end to end incident life cycles • Continually monitor 'value for money', deliverables and the business derived • Regularly check for supplier dependencies - ensure all procedures, functions and processes are clearly documented, up-to-date and available • Make certain that the contractual terms, deliverables and chargeable activities are clearly understood and agreed by both parties • Provide guidance or supply on integrating the incident management toolset(s) • Notification of changes relating to Post Office Limited (POL) with direct impact to the Suppliers • Provide telephony system for the SPOC IVR
CM (Supplier - Post Office)	• Own internal Incident Management Process

POL00394097

	• Provide the services outlined to NS in SLAs • Provide Management Reporting to NS • Manage alerting and escalations of incidents within the area
EDS (Supplier - 3rd Party)	• Owns internal Incident Management Process • Provide Management Reporting to NS • Manage alerting and escalations of incidents within the area
TSD (Supplier - 3rd Party)	• Owns internal Incident Management Process • Provide Management Reporting to NS • Manage alerting and escalations of incidents within the area
Vendor Reporting Into TSD (Supplier - 3rd Party)	• Owns internal Incident Management Process • Provide Management Reporting to TSD • Manage alerting and escalations of incidents within the area
Telephony (Supplier - 3rd Party)	• Owns internal Incident Management Process • Provide Management Reporting to NS • Manage alerting and escalations of incidents within the area

2.1.1.3 Process Inputs:

- Business Requirements
- Management Reporting
- Service Requirements
- Post Office Guidelines on Standards
- Training Needs
- Integrated Service Management Tool Set
- Organisational and Business Changes

2.1.1.4 Process Outputs:

- A service where logging of all POL's incidents are on an Incident Management system
- A service, which has POL's incidents, logged quickly and correctly
- A service which provides an effective resolution of all reported Incidents
- Complete and accurate incident quality records
- Escalation as required in accordance with Priority, Service Level Agreements or business impact as stated by NS
- Incident desk performance metrics as defined by NS
- Management Information/reports as defined by NS
- Performance reports against formal target (Service Level Agreements **SLA's**)

POL00394097

2.1.1.5 Recommended Key Performance Indicators (KPI's)

Listed below are metrics that can be utilised for Key Performance Indicators:

- Mean time to pick up call from service desk call queues
- Abandonment rate of telephone calls
- Call volumes per service desk analyst
- Percentage reduction in average time to respond to a call assistance from the first-line operatives
- Percentage increase in the incidents resolved by first line operatives
- Percentage increase in the incidents resolved by first line operatives on first response
- Percentage reduction of incidents incorrectly assigned
- Percentage reduction of incidents incorrectly categorised
- Reduced mean elapsed time for resolution or circumvention of incidents broken down by impact code
- Increased percentage of incidents resolved within agreed (in SLAs) response times by impact code
- Reduction in the service unavailability caused by incidents
- Increased percentage of incidents resolved within target times by priority
- Increased percentage of incidents resolved within target times by category
- Percentage reduction in the average time for the second line 3rd party vendor to respond
- Reduction of incident backlog
- Percentage reduction in incidents reopened
- Percentage reduction in the overall average time to resolve incidents
- Reduction in the number of incidents requiring more than one second line 3rd party vendor
- Percentage reduction in average cost of handling incidents
- Improved percentage of the business incidents dealt with first line operatives
- Percentage improvement in average number of incidents handled by each first line operative
- No delays in the production of management reports
- Improved scores on the Customer Satisfaction Surveys CSS
- Percentage improvements in CSS responses on the Incident Management Service
- Percentage reduction in the length of queue time waiting for Service Desk response
- Percentage reduction in the number of lost Service Desk calls
- Percentage reduction of the number of the revised business instructions issued

POL00394097

2.1.2 Problem Management

The Network Banking Support Centre (NBSC) will be responsible and have ownership for the Problem Management process for both reactive and proactive Problem Management.

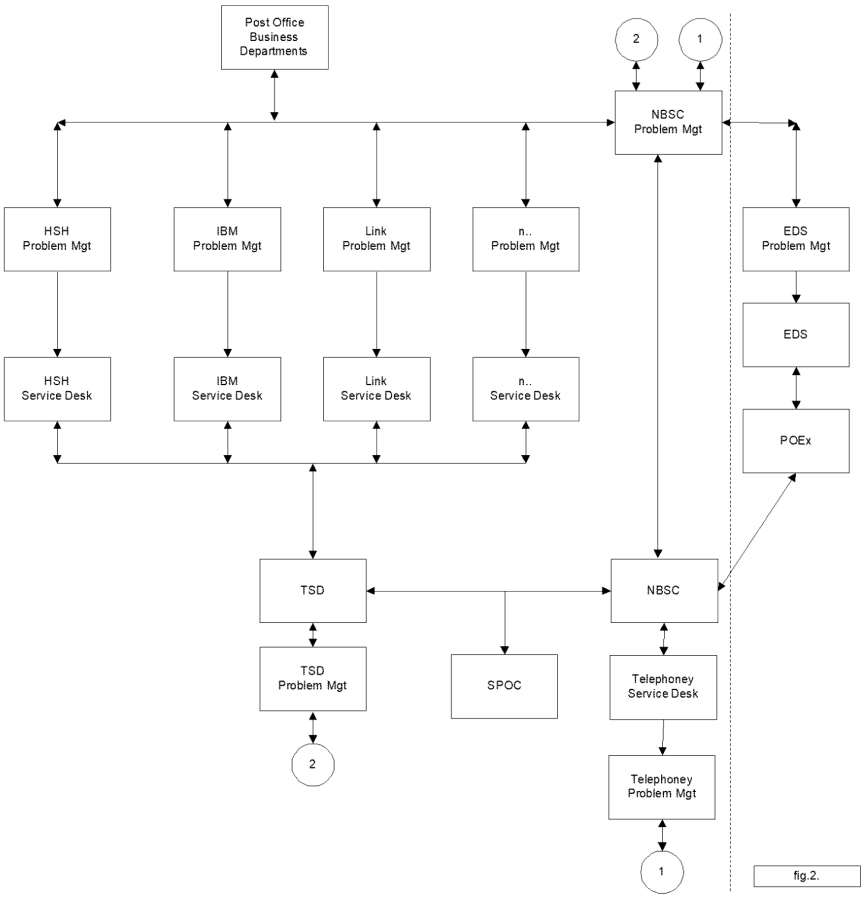


fig.2.

It is envisaged that the NBSC Problem Management team will be the central point of contact for all suppliers and business areas impacted by either an IT or Business problem. NBSC Problem Management will manage reactively by utilising a Major Incident Team and Major Incident process. It will manage proactively Problem Management through Problem Management forums.

The Major Incident Teams will consist of the NBSC Problem Manager and identified members of POL staff that are required to effectively manage the Incident. Possible team members would be departmental representatives for Public Relations, Fraud, Service Desk(s) Team Leaders, 3rd Party Problem Managers (where appropriate) and Representatives of Technical Teams responsible for the investigation of the incident. Due to the distributed nature of

POL00394097

POL and it's suppliers this will be a virtual team as opposed to a team that can be brought together on-site.

The Problem Management forum will be a team responsible for co-ordinating, tracking and monitoring the outstanding issues effecting Network Banking. These problems will include on-going investigations into root causes following Major Incidents. The Problem Management Forum would also be responsible to reviewing Incident Management Trend data and agreeing if investigations are required into emerging trends. Where the investigations into emerging trends are agreed the Problem Management forum will co-ordinate, track and monitor the outstanding issues.

2.1.2.1 Scope of process:

Problem Management will be responsible for all Problems throughout their life cycle; this will include high Priority Incidents from both business and IT related. The function will be responsible for controlling and managing all Problems and maintaining a Known Errors database. Problem Management will not own Incidents, but will be responsible for their resolution if escalated. Problem Management should be a reactive and proactive function.

2.1.2.2 Roles & Responsibilities (Post Office & Supplier):

The following suggested list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles required within the Problem Management function. Roles and responsibilities similar to these should also exist within each of the technical solution suppliers and the interfaces between the supplier and POL should be clearly defined:

Role	Responsibilities
NS (Post Office - Customer)	• Own the Problem Management framework process flow for end to end Problem life cycles • Regularly check for supplier dependencies - ensure all procedures, functions and processes are clearly documented, up-to-date and available • Establish and maintain the Problem Management Forum • Establish and maintain a problem and known error databases • Make certain that the contractual terms, deliverables and chargeable activities are clearly understood and agreed by both parties • Provide guidance or supply on integrating the problem management toolset(s)
Problem Management for Suppliers - 3rd Party & CM - Post Office	• Owns it's internal Problem Management Process • Provide Management Reporting to NS Problem Management • Manage alerting and escalations of incidents within it's area

POL00394097

2.1.2.3 Process Inputs:

- Business Requirements
- Management Reporting
- Post Office Guidelines on Standards
- Training Needs
- Integrated Service Management Tool Set

2.1.2.4 Process Outputs:

- Management Reporting
- Problem Management Forum Agendas
- Major Incident Reports
- Maintenance of Known Error Databases

2.1.2.5 Recommended KPI's:

Listed below are metrics that can be utilised for Key Performance Indicators:

- Percentage reduction in repeat Incidents/Problems
- Percentage reduction in Incidents and Problems affecting service to Customers
- Percentage reduction in known Incidents and Problems encountered
- No delays in production of management reports
- Improved Customer Satisfaction Survey response on business disruption caused by Incidents and Problems
- Percentage reduction in average time to resolve Problems
- Percentage reduction of the average time to implement fixes
- Percentage reduction of the average time to diagnose Problems
- Percentage reduction of the average number of undiagnosed Problems
- Percentage reduction of the average backlog of open Problems and errors
- Percentage reduction of the impact of the Problems and User
- Reduction in the business disruption caused by Incidents and Problems
- Percentage reduction in the number of Problems escalated (missed target)
- Increased percentage of proactive Changes raised by the Problem Management, particularly from Major Incidents and Problem Reviews

POL00394097

2.1.3 Configuration Management

Technical Configuration Management should be wholly owned and managed for POL by the TSD with SLAs detailing the level and frequency of Configuration Management information required by POL. The main objectives of the managed Configuration Management process are to ensure the following:

- The accounting for all the IT assets and configurations within the NB arena
- The provision of accurate information on configurations and their documentation to support all other POL Service Management processes
- The provision of a sound basis for Incident Management, Problem Management, Change and Release Management
- Verification of the configuration records against the infrastructure and correction of any exceptions on behalf of POL.

It is expected that the technical solution suppliers (i.e. IBM, Fujitsu Services, Link, Business Systems, etc) will have their own Configuration Management systems and procedures. It will be the role of the TSD to amalgamate this information to provide POL with a single snapshot of the overall technical network solution / configuration as required.

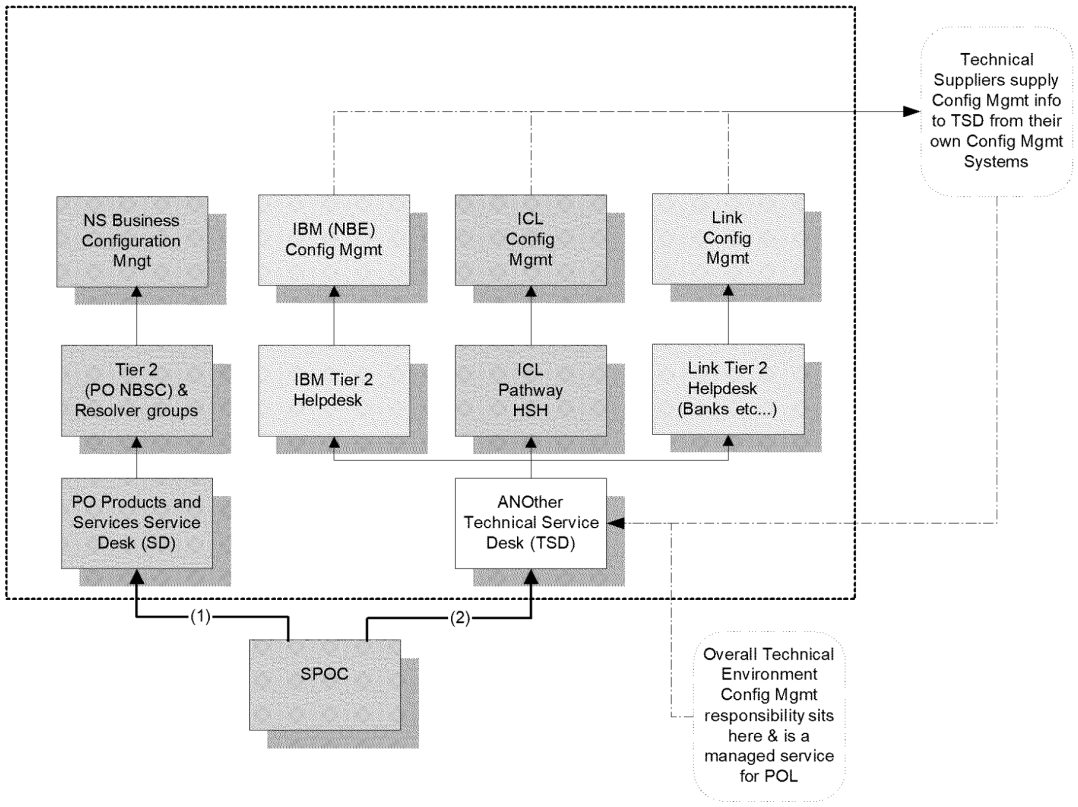
It is also the responsibility of the TSD to ensure that appropriate procedures are in place (between themselves and POL) to ensure the regular and appropriate communication of any changes within the network environment (all 3rd party supplier changes affecting POL should be picked up within the POL Change Management process). This should then act as a guarantee that the snapshot they provide to POL is up to date within an understood and agreed timeframe.

Where technical Configuration roles and databases currently exist within POL a more in depth review is necessary to understand what value these internal support functions add, or whether they are simply a duplication of effort.

Existing business focused Configuration Management processes and the Network Support CMDB do not necessarily need to be handed over to the TSD. However to provide POL with an overall view of all Configuration Items (CIs), technical and non-technical, consideration must be given to the introduction of an appropriate support tool solution – whether fully integrated or simply compatible. Any CMDB should be able to hold the relationships between all suppliers' system components, including Incidents, Problems, Known Errors, Changes and Releases.

POL00394097

The diagram below shows the involved suppliers, the internal teams and the required interfaces to the managed Configuration Management process



2.1.3.1 Scope of process:

TSD will be responsible for providing POL with the necessary technical Configuration Management information for all direct suppliers to POL across the Network Banking infrastructure. This information will be provided to POL within an agreed timescale and to an agreed format.

It is the responsibility of POL to ensure that appropriate interfaces exist between the technical CMDB and any non-technical configuration databases within the organisation. Ideally these would be combined to provide a single repository for all POL CI information aiding infrastructure management and control.

2.1.3.2 Roles & Responsibilities

The following list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles required within the technical Configuration Management function. Roles and responsibilities similar to these should also exist within each of the technical solution suppliers:

POL00394097

Role	Responsibilities
Configuration Manager –	• Works to the overall objectives agreed with the IT Services Manager; implements the organisation's Configuration Management policy and standards. • Evaluates existing Configuration Management systems and the design, implementation and management of new/improved systems for efficiency and effectiveness – including estimating and planning the work and resources involved, and monitoring and reporting on progress against plan. • Proposes and agrees scope of the Configuration Management processes, function, the items that are to be controlled and the information that is to be recorded. Develops Configuration Management standards, plans and procedures. • Mounts an awareness campaign to win support for the new Configuration Management procedures. Ensures that changes to the Configuration Management methods and processes are properly approved and communicated to staff before being implemented. Plans, publicises and oversees implementation of new Configuration Management systems. • Arranges recruitment and training of staff. Trains Configuration Management specialists and other staff in Configuration Management principles, processes and procedures. • Evaluates proprietary Configuration Management tools and recommends those that best meet the organisation's budget, resource, timescale and technical requirements. Directly or indirectly customises proprietary tools to produce effective Configuration Management environments in terms of databases and software libraries, workflows and report generation. • Creates and manages the Configuration Management plan, principles and processes and their implementation. This includes CI registration procedures internal and 3rd party interface procedures); access controls and privileges. Ensures that the correct roles and responsibilities are defined in the Configuration Management plans and procedures. • Proposes and agrees CIs to be uniquely identified with naming conventions. Ensures that staff comply with identification standards for object types, environments, processes, life-cycles, documentation, versions, formats, baselines, releases and templates.

POL00394097

	• Proposes and/or agrees interfaces with Change Management, Problem Management, Network Management, Release Management, computer operations, logistics, finance and administration functions. • Plans and executes population of the CMDB. Manages and maintains CMDB, central libraries, tools, common codes and data. Ensures regular housekeeping of the CMDB. • Provides reports, including management reports (indicating suggested action to deal with current or foreseen shortcomings), impact analysis reports and configuration status reports. • Uses or provides the CMDB to facilitate impact assessment for RFCs and to ensure that implemented changes are as authorised. Creates change records, configuration baselines, and package release records in order to specify the effect on CIs of an authorised change. Ensures any changes to change authorisation records are themselves subject to Change Management procedures. Ensures that the CMDB is updated when a change is implemented. • Provides the CMDB to help identify other CIs affected by a fault that is affecting a CI. • Performs configuration audits to check that the physical IT inventory is consistent with the CMDB and initiates any necessary corrective action. • Initiates actions needed to secure funds to enhance the infrastructure and staffing levels in order to cope with growth and change. • Assists auditors to audit the activities of the Configuration Management team for compliance with laid-down procedures. Ensures corrective action is carried out.
Configuration Librarian –	• to control the receipt, identification, storage, and withdrawal of all supported CIs to provide information on the status of CIs to number, record, store and distribute Configuration Management issues • assist Configuration Management to prepare the Configuration Management Plan • create an identification scheme for Configuration Management libraries and the DSL • create libraries or other storage areas to hold CIs • assist in the identification of products and CIs • maintain current status information on CIs • accept and record the receipt of new or revised configurations into the appropriate library • archive superseded CI copies

POL00394097

	• hold the master copies • issue copies of products for review, change, correction or information when authorised to do so • maintain a record of all copies issued • notify holders of any changes to their copies • collect and retain information that will assist in the assessment of what CIs are impacted by a Change to a product • produce configuration status accounting reports • assist in conducting configuration audits • Liaise with other Configuration Libraries where CIs are common to other systems.

The following list of inputs and outputs to the Configuration Management process is not exhaustive but is designed to give a clear indication of the requirement:

2.1.3.3 Inputs:

- POL Configuration Management Reporting Requirements
- POL Change Management Process
- POL Requests for Change
- 3rd Party Supplier Requests for Change
- Supplier Configuration Management process information & data
- Forward Schedule of Changes
- Supplier contracts (Configuration & Change Management sections as a minimum).
- Supplier Service Level Agreements (Configuration & Change Management sections as a minimum).
- Service Management components and records such as capacity plans, IT service continuity plans, Incidents, Problems, Known Errors, etc.

2.1.3.4 Outputs:

- Management Reporting from TSD to relevant resources at POL (e.g. Capacity Manager, Change Manager…)
- Results of configuration audits
- A statement of the objectives and goals of the Configuration Management team.
- A single snapshot of entire NB technical infrastructure

2.1.3.5 Recommended Critical Success Factors (CSF's) and KPI's:

The main critical success factors and the contributing key performance indicators for the E2E NB Configuration Management function are listed below:

2.1.3.5.1 CSF 1: IT Asset Control

- There is a percentage reduction in the number of Configuration Item (CI) attribute errors found in the Configuration Management Database (CMDB)
- There is a percentage increase in the number of CIs successfully audited

POL00394097

- There are percentage improvements in the speed and accuracy of audits.

2.1.3.5.2 CSF 2: The process effectively supports the delivery of quality IT services.

- There is a percentage reduction in service errors attributable to wrong CI information
- There is an improved speed of component repair and recovery
- Customer satisfaction with services and terminal equipment is improved

2.1.3.5.3 CSF 3: Economic Service Provision

- There is a reduction in the number of 'missing and duplicated' CIs
- There is a better overall understanding of the NB environment and associated maintenance costs and licence fees for which POL is charged

2.1.3.5.4 CSF 4: Support, integration and interfaces to all other IT Service Management processes.

- Percentage reduction of change failures as a result of inaccurate configuration data
- Improved incident and problem resolution time due to the availability of complete and accurate configuration data
- More accurate results from Risk Analysis audits due to available and accurate asset information

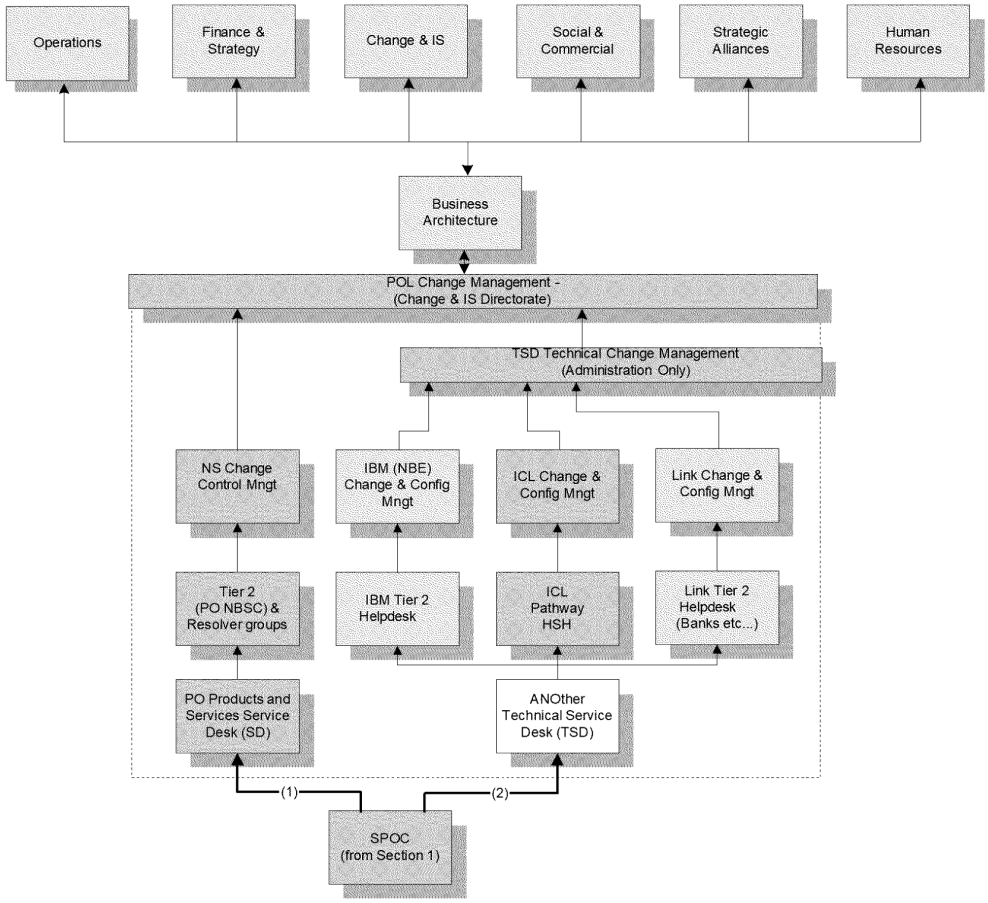
2.1.4 Change Management

The goal of the Change Management process is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the organisation.

Due to the potential of any changes (either internal or external) causing an adverse business impact, it is recommended that POL take overall responsibility for pulling together each of the individual Supplier Change Management functions.

The diagram below shows the interfaces between Change Management, POL and 3rd party suppliers:

POL00394097



It is expected that each technical solution supplier (i.e. IBM, Fujitsu Services, Link, BS, etc) will have their own Change Management systems and procedures that comply with the expectations of POL. However, it will be the role of Change Management within POL (Change and IS Directorate) to bring together all Change Information supplied by 3rd party suppliers (through the TSD) and to ensure appropriate Change Management controls and procedures protect the day to day POL business and emerging strategies. This involves not only co-ordinating changes intended by third parties but also providing a Change Management interface with the business considering any potential clashes with internal business changes, product releases, business strategy, etc.

It is also the responsibility of POL Change Management to ensure that 3rd party supplier Change Management procedures are aligned with their own. It is the responsibility of both parties and the TSD to ensure that the appropriate authorisation routes are understood and agreed for changes of all types (standard, non-standard and emergency) and that these are fully and clearly documented.

In order to facilitate the process of effective 'holistic' Change Scheduling, it is the responsibility of POL Change Management (Change and IS Directorate) to co-

POL00394097

ordinate and own the production and distribution of a 'Forward Schedule of Change' (FSC) and a 'Projected Service Availability' (PSA). The latest versions of these documents should be available to everyone within the organisation, preferably contained within a commonly available internet or intranet server. The FSC should contain details of all the Changes approved for implementation and their proposed implementation dates. The PSA should contain details of Changes to agreed SLAs and service availability because of the currently planned FSC. These documents should be agreed with the relevant Customers / Stakeholders within the business, with Service Level Management (Supplier & Service Performance Team), with the NBSC, TSD and with Availability Management. Once agreed, the NBSC should communicate any planned additional downtime to the User community at large, using the most effective methods available and with close collaboration with the Change owner(s).

There should be one overall Change Management function within POL responsible for pulling together ALL Change Initiatives whether business, technical or otherwise focussed and feed-ins to this team should be well documented, distributed and communicated throughout the organisation. It is important to have senior management support for the Change process and for the overseeing POL Change Mgmt function (Change and IS) in order for it to have any authority.

It is also paramount that the appropriate support tool is used, preferably a centrally based Configuration Management Database (CMDB), to log and to manage all Changes. Such a tool should have the following facilities:

- Requests For Changes (RFCs) and Problem Records (PRs) stored upon the same database, in an easily accessible format
- the ability to identify the relationship between RFCs, PRs and Configuration Items (CIs)
- the capability to link RFCs to projects
- the means to identify easily the other CIs that will be impacted whenever a Change to any specific CI is proposed
- automatic production of requests for impact and resources assessment to the 'owners' of the impacted CIs
- the ability for all authorised personnel to submit RFCs from their own terminal or location
- the ability to 'progress' requests through the appropriate stages of authorisation and implementation and to maintain clear records of this progress
- the ability to allow Change Management staff, Change builders, testers, etc to add text to Change records
- clear definition of back-out procedures should a Change cause problems
- automatic warnings of any RFCs that exceed pre-specified time periods during any stage
- automatic prompting to carry out reviews of implemented Changes
- automatic generation of management and trend information relating to Changes
- the ability to build Changes
- automatic production of FSCs

POL00394097

- A process/workflow feature.

2.1.4.1 Scope of process:

End to End Change Management includes the management and co-ordination of Change processes relating to:

- hardware
- communications equipment and software
- system software
- products and services
- 'live' applications software
- all associated documentation and procedures

This means that changes to any components that are under the control of an applications development project - for example, applications software (i.e. Horizon), documentation or procedures - do not come directly under Change Management but would be subject to project Change Management procedures. The E2E Change Management team will, however, be expected to liaise closely with Release Management project managers and Operational Business Change (OBC) staff to ensure smooth implementation and consistency within the changing management environments.

2.1.4.2 Roles & Responsibilities (Post Office & Supplier):

The following suggested list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles required within the Change Management function. Roles and responsibilities similar to these should also exist within each of the technical solution suppliers and the interfaces between the supplier, TSD and POL should be clearly defined:

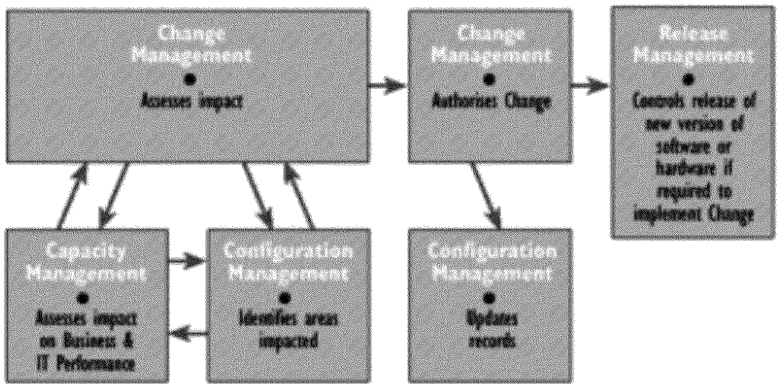
Role	Responsibilities
POL Overall Change Manager (Change & IS Directorate)	• Develop and maintain the overall Change Management process and ensure appropriate interfaces and contractual inclusion between POL, TSD and 3rd party suppliers • Mount awareness campaign to gain support • Chair the Change Advisory Board (CAB) • Ensure the Change Process is adhered to throughout the organisation and that contractual obligations are met by the suppliers • Perform on-going monitoring of changes as appropriate • Review Change Management procedures • Management Reporting
POL Overall Change Management Team (Change & IS Directorate)	• Direct and co-ordinate all Changes through the established process • Schedule ALL Changes and Releases • Distribute FSC and manage communications to the Customer via NBSC • Liaise with Change Builder / individual team

POL00394097

	Change Manager • Assemble Changes into release packages • Perform a post implementation review on any changes not reviewed at individual team level • Compare actual cost of the change with budgeted costs • Liaise with Release Management over distribution of software changes • Liaise with Customers over acceptable timing of changes • Perform on-going monitoring of changes as appropriate • Review Change Management procedures
Change Manager – Individual Team Level (e.g. OBC, NS & TSD)	• Develop and maintain the Change Management process within the team, ensuring alignment and communication pathways are established into overall POL Change Management Team (Change & IS) • Mount awareness campaign to gain company & management support • Direct and co-ordinate all Changes through the established process • Schedule Changes • Liaise with Change builder • Ensure adequate testing has been carried out • Check and approve back-out plans • Assemble Change into release packages • Ensure resources are available to carry out changes • Perform a post implementation review on all changes • Compare actual cost of changes with budgeted costs and feed into Change and IS Directorate • Liaise with Release Management to arrange for the release of code from the Definitive Software Library (DSL) where appropriate • Liaise with Release Management over the distribution of software changes • Liaise with Customers over acceptable timing of changes • Obtain documentation and sign-off from supplier/change builder before implementation • Authorise releases into live environment • Initiate back out plans if the change fails • Perform on-going monitoring of changes as appropriate • Review Change Management procedures

POL00394097

Change Management is not responsible for identifying components affected by change or updating change records (this is the domain of Configuration Management), nor is it responsible for the Release of new or changed components (the domain of Release Management). The relationships between Capacity Management, Change Management, Configuration Management, and Release Management are illustrated below.



2.1.4.3 Inputs:

Inputs to the Change Management process will comprise:

- RFCs
- CMDB
- Forward Schedule of Changes (FSC)

Activities undertaken will involve:

- filtering changes
- managing changes and the change process throughout POL
- Co-ordinating 3rd Party Supplier and internal changes
- chairing the CAB and the CAB/Emergency Committee
- reviewing and closing RFCs
- Management reporting.

2.1.4.4 Outputs:

- FSC
- RFCs
- CAB minutes and actions
- Change Management reports.

POL00394097

2.1.4.5 Recommended CSF's and KPI's:

The main critical success factors and the contributing key performance indicators for the E2E NB Change Management function are listed below:

2.1.4.5.1 CSF 1: Provision of a repeatable process for making technical Changes

- There is a percentage reduction in rejected Change Requests (CRs)
- There is a percentage reduction in the number of unauthorised changes
- There are percentage improvements in the number of Change Requests implemented on time
- There is a percentage reduction in the average time to make changes
- There are fewer changes 'backed out' due to testing failures
- There is a percentage reduction in changes required due to previous change failures

2.1.4.5.2 CSF 2: The ability to make changes quickly and accurately, with effective co-ordination between POL and other supplying Change Management teams.

- There is a percentage reduction in the number of urgent changes
- There is a percentage reduction in the number of urgent changes causing incidents
- There is a reduction in the percentage of changes implemented without being tested
- There is a percentage reduction of urgent changes requiring back-out
- There is a reduction of urgent or high priority changes submitted without business case to justify the decision
- There are improvements in the change communication speed amongst relevant change groups
- There is a higher percentage of correct authorisation procedures being followed first time

2.1.4.5.3 CSF 3: The protection of services when making a change

- There is a reduction in both the scheduled and unscheduled service unavailability caused by changes
- There is a percentage reduction in 'backed out' changes
- There is a percentage reduction of unsuccessful changes
- There is a percentage reduction in changes causing incidents
- There is a percentage reduction in changes impacting core service time and SLA service hours
- There is a percentage increase in changes activated outside core service time and SLA service hours
- There is a reduction in the percentage of changes not referred to a Change Advisory Board (CAB) or Change Advisory Board Emergency Committee (CAB/EC)
- Improvement in any Customer Satisfaction Survey (CSS) feedback on change

POL00394097

- Percentage reduction in failed changes that do not have recorded back-out plan
- Percentage reduction in time to implement a change freeze

2.1.4.5.4 CSF 4: The ability to show efficiency and effectiveness results

- There is a percentage efficiency improvement based on number of Change Requests processed
- There is a percentage increase in the accuracy of change estimates (time and cost)
- There is a percentage reduction in the average cost of handling a change
- There is a percentage reduction in change overtime due to better planning and co-ordination across NB environment
- There is a reduction in the 'cost' of failed changes
- There is an increased percentage of changes implemented on time
- There is an increased percentage of changes implemented to budget
- There is a reduction in the percentage of failed changes
- There is a reduction in the percentage of backed out changes

2.1.5 Release Management

As with Change Management, due to the potential of any Releases (either internal or external) causing significant adverse business impact it is recommended that POL take overall responsibility for pulling together each of the individual Supplier Release Management functions, ensuring minimal conflict.

It is expected that each technical solution supplier (i.e. IBM, Fujitsu Services, Link, BS etc) will have their own Release Management systems and procedures that comply with the expectations of POL. However, it will be the role of Release Management within POL to bring together all Release Information supplied by 3rd party suppliers and to ensure appropriate Release Management controls and procedures protect the day to day POL business and emerging strategies.

The overall goals of POL Release Management should be to:

- plan and oversee the successful rollout of software and related hardware within POL
- design and implement efficient procedures for the distribution and installation of changes to IT systems
- ensure that hardware and software being changed is traceable, secure and that only correct, authorised and tested versions are installed
- communicate and manage expectations of the customer during the planning and rollout of new releases
- agree the exact content and rollout plan for the release, through liaison with POL Change Management
- implement new software releases or hardware into the operational environment using the controlling processes of Configuration Management and Change Management - a release should be under Change Management and may consist of any combination of hardware, software, firmware or document CIs

POL00394097

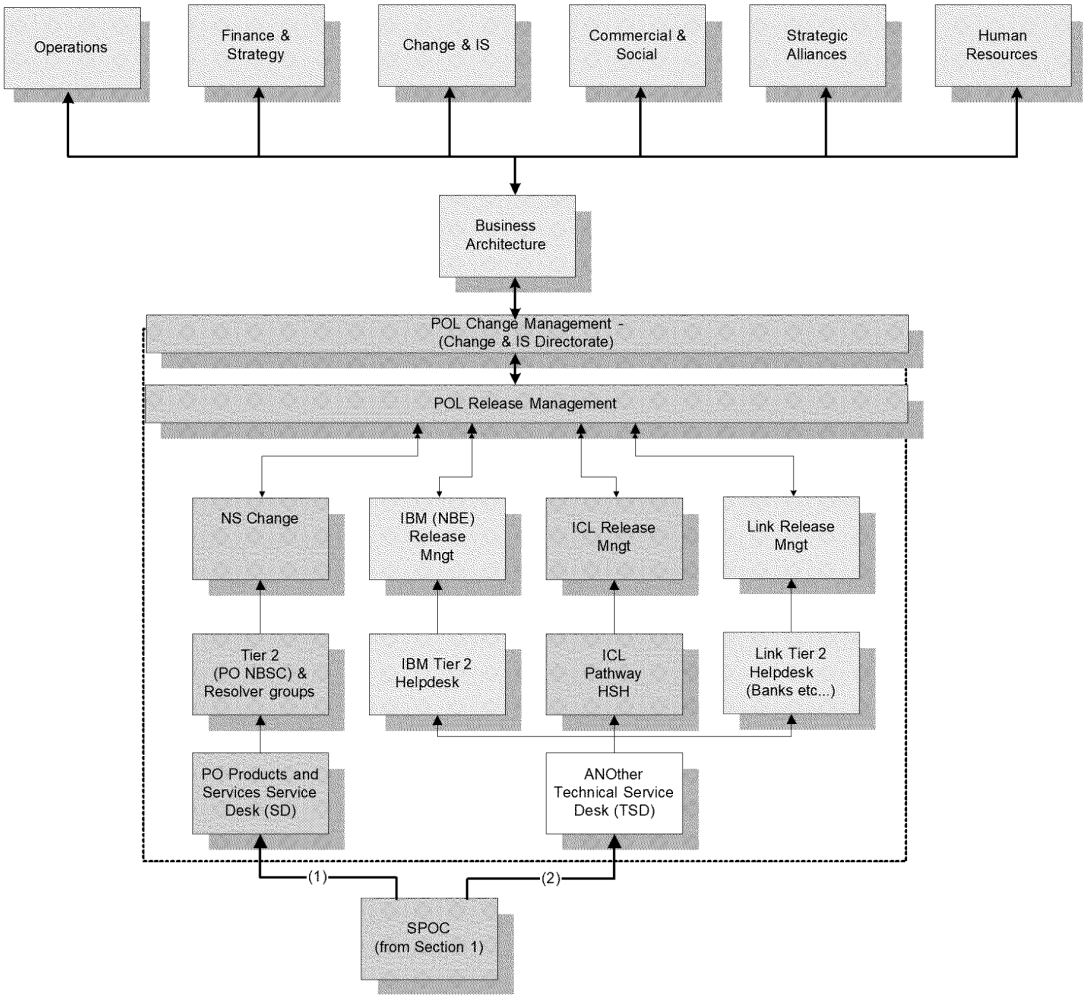
- ensure that master copies of all software are secured in the Definitive Software Library, RDS (either on POL site, or on behalf of POL) and that the Configuration Management Database (CMDB) is updated
- Ensure that all hardware being rolled out or changed is secure and traceable, using the services of Configuration Management.

The focus of POL Release Management should be the protection of the live environment and its services through the use of formal procedures and checks and the successful co-ordination of all 3rd party suppliers.

POL Release Management must work closely with POL Change Management and Configuration Management processes to ensure that a shared CMDB is kept up-to-date following Changes implemented by new Releases, and that the content of those Releases is stored in the DSL (Business Systems Reference Data System).

POL00394097

The diagram below shows the interfaces between Release Management, POL and 3rd party suppliers:



2.1.5.1 Scope of process:

POL Release Management should undertake the planning, design & build (where appropriate), configuration and testing of hardware and software to create a set of release components for the live POL environment. Activities should also cover the planning, preparation and scheduling of a release to the many POL customers and locations.

Overall POL Release Management activities should include and / or ensure:

- release policy and planning
- release design, build and configuration (where appropriate)
- release acceptance, in conjunction with OBC teams

POL00394097

- rollout planning (in conjunction with POL Change Management and 3rd party suppliers)
- extensive testing to predefined acceptance criteria, in conjunction with OBC teams
- sign-off of the release for implementation
- communication, preparation and training (through NS Change Control & NBSC)
- audits of hardware and software prior to and following the implementation of changes (in conjunction with TSD Configuration Management)
- installation of new or upgraded hardware
- storage of controlled software in both centralised and distributed systems
- Release, distribution and the installation of software (or the management of 3rd parties carrying out this role.

The main components to be controlled by POL Release Management are:

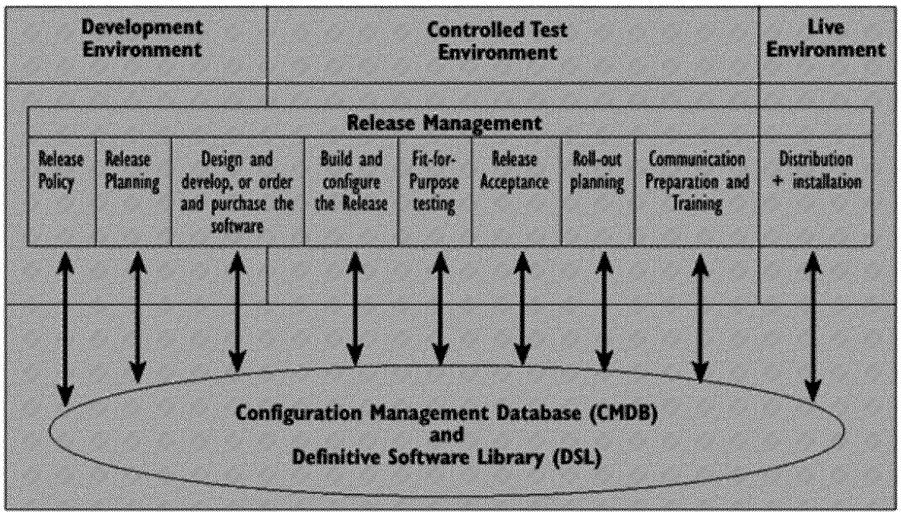
- application programs developed in-house
- externally developed software (including standard off-the-shelf software as well as customer-written software)
- utility software
- supplier-provided systems software
- hardware, and hardware specifications
- Assembly instructions and documentation, including User manuals.

Release Management should be used for:

- large or critical hardware rollouts, especially when there is a dependency on a related software Change in the business systems, i.e. not every single PC that needs to be installed
- major software rollouts, especially initial instances of new applications along with accompanying software distribution and support procedures for subsequent use if required
- Bundling or batching related sets of Changes into manageable-sized units.

The following diagram outlines the major activities in Release Management and their position in the life-cycle of a change. Configuration Management records should be updated during the build and release to ensure that trusted releases exist and can be reverted to in case of problems. This then requires a sound communication process between POL Release Management and the TSD Configuration Management function. A release should be carried out under Change Management and the content and timing of a release should be authorised in advance via the Change Management process.

POL00394097



2.1.5.2 Roles & Responsibilities (Post Office & Supplier):

It is the role of the POL Release Manager to measure, and push for improvements in the KPI's with 3rd party suppliers and to co-ordinate all releases for POL, working closely with the overall Change Manager.

Below is a suggested list of activities to be the responsibility of the overall POL Release Manager. His / her work should be in conjunction with any other 'release teams' within POL (e.g. NS OBC) and / or 3rd party suppliers (e.g. Business Systems – BS):

- Gaining consensus on the release contents
- Agreeing to the phasing over time and by geographical location, business unit and customers
- Producing a high-level release schedule
- Conducting site surveys to assess existing hardware and software in use
- Planning resource levels (including staff overtime)
- Agreeing on roles and responsibilities (especially between POL teams and 3rd party suppliers). These must be documented and easily accessible to the organisation
- Obtaining detailed quotes and negotiating with suppliers for new hardware, software or installation services
- Producing back-out plans
- Developing a quality plan for the release
- Planning acceptance of support groups and the customer.

2.1.5.3 Inputs

Inputs to the Release Management process will comprise:

- RFCs

POL00394097

- CMDB
- Forward Schedule of Changes (FSC)

2.1.5.4 Outputs:

- Release Schedule
- RFCs
- Management reports

2.1.5.5 Recommended CSF's and KPI's:

The main critical success factors and the contributing key performance indicators for the E2E NB Release Management function are listed below:

2.1.5.5.1 CSF 1: Provision of better quality software and hardware

- There is a percentage reduction in the use of software and hardware release that have not passed the required quality checks
- There is a percentage reduction in installed software not taken from the Definitive Software Library (DSL), in POL's case for Horizon the RDS
- There is a percentage reduction in non-standard hardware
- The assurance that all bought-in software complies with legal restrictions
- There is a percentage reduction of unauthorised reversion to previous releases
- There is a percentage reduction in the use of unauthorised software and hardware

2.1.5.5.2 CSF 2: The provision of a repeatable process for rolling out software and hardware releases

- All new Releases are planned and controlled by Release Management
- All installed software is taken from the DSL
- All appropriate hardware in stored in Definitive Hardware Store (DHS)
- There is a percentage reduction in the number of failed distributions of releases to remotes sites
- There is a reduction in the percentage of urgent releases
- There is an increase in the percentage of 'normal release units' as opposed to ad hoc releases

2.1.5.5.3 CSF 3: The swift and accurate implementation of releases, effectively co-ordinated with other business and technical changes

- There is a percentage reduction in build failures
- There is a percentage improvement in 'on-time' implementations of releases to all sites
- There is a percentage reduction in the number of urgent releases
- There is a percentage reduction in releases causing incidents
- There is an overall reduction in the percentage of releases implemented without being tested

POL00394097

- A reduced percentage of urgent or high priority releases requested without the appropriate business case/justification

2.1.5.5.4 CSF 4: Cost effective releases

- There is an increase in the number of releases built and implemented on schedule
- There is an increase in the number of releases built and implemented within budget
- There is a reduction in service unavailability caused by releases
- There is a percentage reduction in releases backed out
- There is a percentage reduction in the number failed releases
- There is a percentage reduction in the average cost of handling a release
- An increase in the number of planned composition of releases matching actual composition (demonstrating good release planning)
- There will be no evidence of unnecessary duplication in release building (e.g. multiple builds of remote sites, when copies of a single build would suffice)
- There is a percentage increase in the accuracy of release estimates (required time, cost & resources)

2.1.6 Capacity Management

The Capacity Management (CM) process for the Network Banking (NB) environment should be owned by a NS on behalf of POL

In the past the majority of the information regarding capacity planning within POL related to the capacity within the business environment in terms of numbers of Post Offices, numbers of staff in the offices etc. In the future, more technical environment of NB, there will be an increased necessity to convert this information into planning information that can relate to the IT infrastructure within each supplier domain. This can then be used by each IT supplier e.g. IBM, EDS etc. to plan their infrastructure.

The future Capacity process should therefore encompass:

1. The monitoring of performance and throughput of IT services and the supporting infrastructure components.
2. Undertaking tuning activities to make the most effective and efficient use of existing resources.
3. Understanding the demands currently being made for IT resources and producing forecasts for future resources.
4. Influencing the demand for resource, perhaps in conjunction with financial management
5. The production of a Capacity Plan which will enable the IT service providers to provide service of the quality described in the Service Level Agreements (SLA's)

However, not all of the above will be undertaken by POL, but it is recommended that POL develop a Capacity Plan to include the following:

POL00394097

- Introduction
  - Scope
  - Methods used
- Assumptions made
- Management Summary
- Business scenarios
- Service summary
  - Forecasts etc.
- Resource summary
  - Current and recent usage
  - Resource forecasts
- Options for service improvement
- Cost model
- Recommendations

In Service Management terms there are three sub processes that describe Capacity Management:

- Business Capacity Planning
- Service Capacity Planning
- Resource Capacity Planning

Business Capacity Planning
This sub process is responsible for ensuring that the future business requirements for IT services are considered, planned and implemented. The requirements come from the business plans outlining new services, improvements and growth in existing services etc. In the case of the NB project, this is a new service that will necessitate substantial growth in the existing environment and liaison with new suppliers.

Service Capacity Planning
The focus of this sub process is the management of the performance of the "live" operational IT services used by the customers. It is responsible for ensuring that the performance of all services, as detailed in the targets for SLA's and SLR's are monitored and measured and the collected data is recorded, analysed and reported. This is performed by staff with knowledge of all areas of technology used in the E2E service. In the case of the NB service, each individual supplier will have responsibility to ensure the effective delivery of the service component that they are delivering, but only POL will understand the E2E service that is being delivered and will therefore report against it.

Resource Capacity Planning
This sub process is responsible for the management of the individual components of the IT infrastructure. It is responsible for ensuring that all components within the IT infrastructure are monitored and measured and that the collected data is recorded. Individuals manage the process with specialist knowledge in the particular area of technology. Within the NB service, the suppliers are responsible for ensuring that the capacity is available within their domain and therefore this activity will very firmly sit with the suppliers.

POL00394097

In terms of the capacity process above, POL will be responsible for 2, 4 and 5 in the new environment, with the individual suppliers being responsible for 1 and 3. In broad terms this mean that NS will be responsible for ensuring that adequate and timely information is available to enable the suppliers to plan their IT infrastructure in readiness for future demand. NS should not be directly responsible for IT infrastructure capacity.

2.1.6.1 Scope of process:

Capacity Management within NS will be responsible to ensure that appropriate business data is given to each of its suppliers in a timely manner to ensure that they can plan their IT infrastructure capacity in readiness for any changing demand for service.

The NB service framework is provided via a multi vendor environment and internal business units. The NS CM service will interface with all service providers as listed below:

- Fujitsu Services
- I.B.M.
- LINK
- Alliance and Leicester
- NatWest Bank
- E.D.S.
- Consignia Customer Management (C.C.M.)
- Business Systems Business Unit (B.S.B.U.)
- Post Office Ltd.
- NS Service Management teams.

2.1.6.2 Roles & Responsibilities

The following list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles within the team:

Role	Responsibilities
Capacity Manager	• Promote awareness of the function. • Define a CM strategy. • Ensure that the optimum acceptable levels of capacity are implemented to enable efficient and effective delivery of the service. • Ensure members of the CM team are adequately trained to perform their roles. • Ensure the responsibilities of the CM team are understood and executed.
Capacity Management Team	• Conduct CM maturity assessments of each service provider. • Establish formal interfaces between the CM team and the service providers. • Establish effective trigger/alert mechanisms to ensure CM Incidents are escalated to the CM

POL00394097

	team in good time. • Develop and manage the CM supporting documentation. • Request and review the supplier capacity plans. • Register all CM documentation within the CMDB. • Conduct CM reviews and audits. • Assess the E2E NB environment for risk and where applicable make recommendations for risk reduction measures. • Review the design of the proposed E2E NB environment and make recommendations for Capacity Management

The following list of inputs and outputs to the CM process is not exhaustive but is designed to give a clear indication of the requirement:

2.1.6.3 Inputs:

- Technology
- SLA's/SLR's and Service Catalogue
- Business Plans and Strategy
- IS/IT plans and strategy
- Business Requirements and volumes
- Operational schedules
- Deployment and development plans and programmes
- Forward Schedule of Changes (FSC)
- Incidents and Problems
- Service Reviews
- SLA breaches
- Financial Plans
- Budgets

2.1.6.4 Sub Processes

2.1.6.4.1 Business Capacity Management

- Trend
- Forecast
- Model
- Prototype
- Size
- Document future business requirements

2.1.6.4.2 Service Capacity Management

- Monitor
- Analyse

POL00394097

- Tune and report on service performance
- Establish baselines and profiles of use of services

2.1.6.4.3 Resource Capacity Management

- Monitor
- Analyse
- Run and report on the utilisation of components
- Establish baseline and profiles of use of components

2.1.6.5 Outputs

- Capacity Plan
- Capacity Database
- Baselines and profiles
- Thresholds and alarms
- Capacity reports (regular, ad hoc and exception)
- SLA and SLR recommendations
- Costing and Charging recommendations
- Proactive changes and service improvements
- Revised operational schedule
- Effectiveness reviews
- Audit reports

2.1.6.6 Recommended CSF's and KPI's

2.1.6.6.1 Critical Success Factors:

The main critical success factors and the contributing key performance indicators for the End to End NB business continuity function are listed below:

- Accurate business forecasts
- Knowledge of IT strategy and plans ensuring that the plans are accurate
- An understanding of current and future technologies
- An ability to demonstrate cost effectiveness
- Effective interaction with other processes
- An ability to plan and implement the appropriate capacity to match business needs

2.1.6.6.2 KPI's:

- Resource forecasts
  - timely production of forecasts of resource requirements
  - accurate forecasts of trends in resource utilisation
  - incorporation of business plan into Capacity plan

- Technology
  - ability to monitor performance and throughput of all services and components as appropriate
  - implementation of new technology in line with business requirements (time, cost and functionality

POL00394097

  - the use of old technology does not result in breached SLA's due to problems with support or performance

- Cost effectiveness
  - a reduction in "panic buying"
  - no significant over Capacity that can't be justified in business terms
  - accurate forecasts of planned expenditure

- Plan and implement the appropriate IT Capacity to match business needs
  - reduction in incidents due to poor performance
  - reduction in lost business due to inadequate Capacity
  - new services implemented which match the SLR
  - recommendations made about Capacity are acted upon

2.1.7 Availability Management

The Availability Management (AM) process for the Network Banking (NB) environment should be owned by a central function on behalf of Post Office Limited (POL).

Currently availability is mainly for Fujitsu Services (ICL) to determine, however in the future when there will be multiple suppliers, availability of the systems and services will be key to enabling the E2E delivery of Network Banking. Indeed NB will be a critical business process for POL, with all of the credibility issues that surround such a process.

The future availability process should include the following: -

- Ensure IT services are designed to deliver the levels of availability required by the business.
- Provision of a range of IT availability reporting to ensure that agreed levels of availability, reliability and maintainability are measured and monitored on an ongoing basis.
- Optimisation of the availability of the IT Infrastructure to deliver cost effective improvements that deliver tangible benefits to the business and User.
- A reduction in the frequency and duration of Incidents that impact IT Availability.
- Ensure that shortfalls in IT Availability are recognised and appropriate corrective actions identified and progressed.
- Creation and maintenance of a forward looking Availability Plan, aimed at improving the overall availability of IT services and infrastructure components, to ensure existing and future business availability can be satisfied.

However, there are similarities between Availability and Capacity Management, in that not all of the above will be undertaken by POL, but it is recommended that POL develop an availability plan, as the NB service matures, to include the following:

POL00394097

- Introduction
- Scope
- Supplier domains included
- Actual levels of availability versus agreed levels of availability for NB (as experienced by the user).
- Activities being progressed to address shortfalls in availability of the service. Investment decisions and options with associated costs.
- Details of changing availability requirements for the NB service e.g. 7X24. Documented options and associated costs to meet the requirements
- Any planned Service Outage Analysis (SOA). Should be documented within a Forward Looking Schedule.
- A review of SOA's undertaken to ensure infrastructure is being improved
- The suppliers proactively aiming to improve the availability and investigating new technologies in order to do so. Business benefits to POL should form part of the report (note: such improvements may result in less income to the supplier, but in a true win-win situation the supplier should recommend such technological improvements).

The Availability plan for NB should cover a period of one to two years, with a detailed view for the first 6 months of the service.

2.1.7.1 Scope of process:

The availability process for NB within POL will be concerned with the design, implementation, measurement and management of the IT Infrastructure supporting it, albeit that in the main this will be provided by the suppliers. POL should ensure that the suppliers provide evidence of proactive Availability Management to ensure that the overall availability requirements of NB are consistently met. Therefore Availability Management should:

- Apply to the NB E2E service, as it will be business critical
- Be applied to the suppliers, internal as well as external, that form the IT support (ideally before the SLA is created)
- Consider all aspects of the IT Infrastructure and supporting organisations, which may impact Availability, including; training, skills, policy, process effectiveness, procedures and tools

The NB service framework is provided via a multi-vendor environment and internal business units. The NS Availability Management process will interface with all service providers within the E2E environment including: -

- Fujitsu Services
- I.B.M.
- LINK
- Alliance and Leicester
- NatWest Bank
- E.D.S.
- Consignia Customer Management (C.C.M.)
- Business Systems Business Unit (B.S.B.U.)

POL00394097

- Post Office Ltd.
- NS Service Management teams.

2.1.7.2 Roles & Responsibilities

The following list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles within the team: -

Role	Responsibilities
Availability Manager	• Promote awareness of the function. • Define an AM plan. • Ensure that the suppliers provide optimum availability levels to enable efficient and effective delivery of the service. • Ensure members of the AM team are adequately trained to perform their roles. • Ensure the responsibilities of the AM team are understood and executed.
Availability Management Team	• Conduct AM assessments of each service provider. • Establish formal interfaces between the AM team and the service providers. • Establish effective trigger/alert mechanisms to ensure AM Incidents are escalated to the AM team in good time. • Develop and manage the AM supporting documentation. • Request and review the supplier Availability plans. • Register all AM documentation within the CMDB. • Conduct SOA reviews. • Assess the E2E NB environment for Availability risks and where applicable make recommendations for risk reduction measures. • Review the design of the proposed E2E NB environment and make recommendations for Availability Management

The following list of inputs and outputs to the AM process is not exhaustive but is designed to give a clear indication of the requirement: -

2.1.7.3 Inputs

- Availability requirements of the business for the NB service
- A business impact assessment for the business functions underpinned by the infrastructure supporting NB

POL00394097

- The availability, reliability and maintainability requirements of the IT infrastructure that underpins NB
- Information on IT service and component failure, in the form of incident and problem records, similar to the service provided by the supplier, underpinned by the suppliers Infrastructure
- A wide range of configuration and monitoring data pertaining to NB
- Service level achievements against agreed targets for the NB service

2.1.7.4 Outputs

- Availability and recovery design criteria for the NB service
- Details of the availability techniques that each supplier will deploy to provide additional infrastructure resilience to prevent or minimise the impact of component failure to the NB service
- Agreed targets of availability, reliability and maintainability for the IT infrastructure components that underpin NB service
- Agreed targets of availability, reliability and maintainability to reflect the business, User and IT supporting organisation perspectives
- The monitoring requirements for IT components to ensure that deviations in availability, reliability and maintainability are detected and reported
- Availability plan for the proactive improvement of the IT Infrastructures within each supplier domain

2.1.7.5 Recommended CSF's and KPI's

Critical Success Factors (CSF's) and Key Performance Indicators (KPI's) for Availability Management can be many and varied and need to reflect the customer's view of the service. These need to be developed in conjunction with NS.

2.1.8 Business Continuity Management

The Business Continuity Management (BCM) process for the Network Banking (NB) environment will be owned by Post Office Limited, within the Network Support (NS) team. The main objectives of this process are to:

- Ensure that in the event of a disaster or Main Business Continuity Incident (MBCI) the correct contingency measures can be invoked and the NB service recovered to acceptable levels of operation within the time-scales defined by the business.
- Reduce the impact of failures to the E2E NB Service.
- Reduce the risk of failure within the E2E NB Service.
- Ensure that awareness of the roles, responsibilities and objectives of the NS business continuity process are understood throughout the NB environment.

BCM will interface with all service providers across the multi-vendor environment to ensure that adequate business continuity measures are in place. The diagram below shows the involved suppliers, the internal teams and the required interfaces to the NS BCM process:

POL00394097

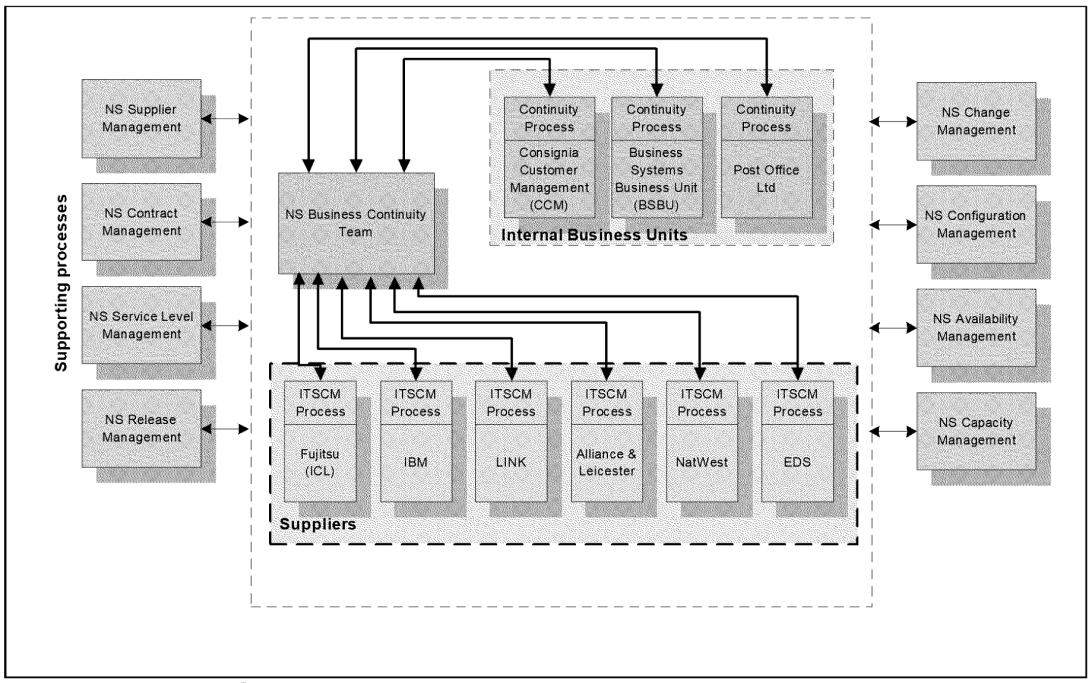


Figure 1 Business Continuity Model for E2E NB

Implementation of the above model will follow the subsequent high-level stages:

Stage 1: Conduct Service Provider BCM Assessments
The BCM team will conduct an assessment of each of the internal and external service providers. This assessment will understand the BC framework within each supplier organisation, measuring it against the required model. This stage will include the receipt, QA and registration of each supplier continuity plan within the NS CMDB.

Stage 2: Definition of the NS E2E Business Continuity Strategy
Following the supplier assessments, an End to End business continuity strategy will be developed which, when implemented, will ensure the required levels of business continuity are delivered across the NB environment.

Stage 3: Establishment of Interface Agreements with each external Service Provider

Interface agreements will be established with each service provider, which are in line with the central BCM strategy. These agreements will build on the contracts already in place, defining the operational interfaces that the supplier organisations must establish with the central BCM process.

Stage 4: Establishment of Interface Agreements with each internal Service Provider.

Interface agreements will be established with the internal service providers, which are in line with the central BCM strategy.

POL00394097

2.1.8.1 Scope of process:

The NS BCM process will be responsible for all activities involved in the provision of continuity measures that are in line with business requirements within the E2E NB service. The NB service framework is provided via a multi-vendor environment and internal business units. The NS BCM service will interface with all service providers as listed below:

- Fujitsu Services
- I.B.M.
- LINK
- Alliance and Leicester
- NatWest Bank
- E.D.S.
- Consignia Customer Management (C.C.M.)
- Business Systems Business Unit (B.S.B.U.)
- Post Office Ltd.
- NS Service Management teams.

2.1.8.2 Roles & Responsibilities

The following list of roles and responsibilities are not exhaustive but are designed to give a clear indication of the roles within the team:

Role	Responsibilities
Business Continuity Manager	• Promote awareness of the business continuity function. • Ensure the minimum acceptable levels of operation for the business are understood. • Define a business continuity strategy. • Implement the business continuity strategy. • Ensure adequate tools and technologies are in place to support the BCM function. • Ensure members of the BCM team are adequately trained to perform their roles. • Ensure the responsibilities of the business continuity team are carried out.
Business Continuity Team	• Conduct business continuity assessments of each service provider. • Provide feedback on the service provider contracts to ensure that adequate provision in made for business continuity. • Establish formal interfaces between the BCM team and the service providers. • Conduct continuity tests and walkthroughs. • Establish effective trigger/alert mechanisms to ensure Main Business Continuity Incidents (MBCIs) are escalated to the BCM team in

POL00394097

	good time. • Develop and manage the business continuity plans. • Develop and manage the business continuity supporting documentation. • Request and review the supplier continuity plans. • Quality Assess all business continuity documentation against POL documentation standards. • Register all business continuity documentation within the CMDB. • Follow change control procedures for all changes to business continuity documentation. • Obtain feedback from each service provider on all conducted continuity tests. Feed this information back into the BCM process. • Conduct business impact analysis (BIA) assessments across the NB service. • Conduct business continuity reviews and audits. • Assess the E2E NB environment for risk and where applicable make recommendations for risk reduction measures. • Review the design of the proposed E2E NB environment and make recommendations for business continuity.

The following list of inputs and outputs to the BCM process is not exhaustive but is designed to give a clear indication of the requirement: -

2.1.8.3 Inputs

- Supplier contracts (business continuity sections as a minimum).
- Supplier Service Level Agreements (business continuity sections as a minimum).
- Service provider business continuity plans and associated documentation.
- Business requirements of the NB service.
- Change forward schedules.
- Alerts/triggers from the Service Desk and Problem Management processes for main business continuity incidents.
- Post Office Guidelines on Standards.
- The central NS CMDB.

2.1.8.4 Outputs

- Management reporting.
- Risk assessment for the NB service.
- Risk reduction recommendations for the NB service.
- Interface agreements with service providers.

POL00394097

- A statement of the objectives and goals of the BCM team.
- Continuity test schedules.
- Training needs of the business continuity team.

2.1.8.5 Recommended KPI's and CSF's

The main critical success factors and the contributing key performance indicators for the E2E NB business continuity function are listed below:

2.1.8.5.1 CSF 1: In the event of a disaster or Main Business Continuity Incident, services can be recovered to meet the business objectives.

2.1.8.5.2 Contributing KPI's

- Regular audits of the Continuity Plans are conducted to ensure that the agreed recovery requirements of the business can be achieved.
- Achievable service recovery targets are recorded within formal SLAs.
- Regular continuity tests and disaster walkthroughs are planned and conducted.
- IT Service Continuity (ITSC) contracts are negotiated and managed with the service providers.
- There is an overall reduction of risk and the impact of failures within the E2E NB environment.

2.1.8.5.3 CSF 2: Awareness of the business continuity function is promoted throughout the E2E NB framework.

2.1.8.5.4 Contributing KPI's

- Ensure that the requirements of the business continuity process are understood E2E throughout the NB framework.
- Ensure that all service providers and staff are able to respond to an invocation of the business continuity plans.
- The objectives and responsibilities of the BCM process are regularly communicated to the business.
- The objectives and responsibilities of the BCM process are regularly communicated to the service providers.

2.1.9 Service Level Management

The Service Level Management (SLM) process for the Network Banking (NB) environment should be owned by a central function (Network Support) on behalf of POL.

The main objective of this process (in ITIL terms), is to maintain and improve IT service quality, through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and to instigate actions to eradicate poor service – in line with business and/or cost justification.

The future SLM process should ensure that:

POL00394097

- The NB service is designed to meet Service Level Requirements
- It enables improved relationships with satisfied customers.
- All parties to the agreement have a clear view of roles and responsibilities relating to the NB service and that there no misunderstandings or omissions.
- There are specific targets to aim for and against which service quality can be measured, monitored and reported on (if you can't measure it, you can't manage it and if you can't manage it you probably don't care!).
- IT effort is focused on the areas that the business believes are key.
- IT and customers have a clear and consistent expectation of the level of service required from NB. Priorities are agreed and understood.
- Weaknesses are identified through effective service monitoring by the suppliers and so that remedial action can quickly take place.
- Service monitoring by the suppliers also shows where Customers or User actions are causing the faults within NB and identifies where working efficiency and /or training can be improved.
- SLM underpins the supplier management for the NB service
- The SLA could be used for a basis of charging for the NB service and therefore help demonstrate the value that the Customers are getting for their money.

SLM should be totally owned and controlled by POL in the new environment. However, the SLM function may want to get the TSD to collect service data on its behalf from the various suppliers. Although SLM is reasonably mature within NS, the process is concentrated around the Fujitsu Services service. At this present time, the SLM teams have had little involvement in the contract negotiations with the new supplier's e.g. IBM.

Planning for Network Banking

In the new NB world the following planning activities need to take place.

- Appoint the new members of the team. The current staffing will need to be enhanced to support the NB service.
- Define the roles, tasks and responsibilities.
- Produce a Mission Statement for the new team to encourage focus and commitment.
- Define the objectives and scope of the new function
- Start an awareness campaign to win support and advise people of their commitment and attain support.
- Quantify the activities, resources, funding and quality criteria
- Consider implementing a Service Catalogue and agree the SLA structure
- Identify support tools for SLA monitoring. In the case of NB, these will be provided by the relevant suppliers
- Set and agree incident priority levels and escalation paths, with customers, internal and external suppliers. This will have to be done in conjunction with the relevant suppliers' Service Desks and Problem Management functions

POL00394097

2.1.9.1 Scope of process:

Service Level Management will be a key process for NS with the inception of Network Banking. The scope will therefore include, but will not be limited to:

- E2E supply chain management
- Underpinning Contracts
- Operational Level Agreements (Internal and External)
- Service Level Agreements

The NB service framework is provided via a multi vendor environment and internal business units. The NS SLM service will interface with all service providers as listed below:

- Fujitsu Services
- I.B.M.
- LINK
- Alliance and Leicester
- NatWest Bank
- E.D.S.
- Consignia Customer Management (C.C.M.)
- Business Systems Business Unit (B.S.B.U.)
- Post Office Ltd.
- NS Service Management teams.
- Internal Operational teams.

2.1.9.2 Roles & Responsibilities

The following list of roles and responsibilities is not exhaustive but is designed to give a clear indication of the roles within the team:

Role	Responsibilities
Service Level Manager	• Promote awareness of the function. • Define a SLM structure that includes • SLA structure • OLA's with the IT provider • 3rd Party contracts • Negotiates the SLA for NB with Customer • Negotiates the OLA with Service Provider • Creates and maintains a Service Catalogue that NB will form part of • Organises and maintains the regular review process with both the IT Customer and Provider • Conducts annual reviews of the SLM process
Service Level Management Team	• Analyse and review service performance against SLA and OLA • Produces regular reports on service performance and achievement to the

POL00394097

	Customers and IT Provider • Initiate any actions to improve service levels • Act as co-ordination point for any temporary changes to the NB service that are required

The following list of inputs and outputs to the AM process is not exhaustive but is designed to give a clear indication of the requirement:

2.1.9.3 Inputs

- SLM requirements of the business for the NB service
- SLA's
- OLA's
- Underpinning Contracts
- Availability and reliability measures
- Inputs from
    - Change Management
    - Configuration Management
    - Release Management
- Support hours

2.1.9.4 Outputs

- Service reporting and reviewing
- Customer information
- Management information
- Key performance indicators
- Improved customer perception
- Basis for charging

2.1.9.5 Recommended KPI's

- Percentage of services covered by SLA's?
- Underpinning contracts and OLA's in place for all SLA's and for what percentage?
- Are SLA's being monitored and are regular reports produced?
- Are review meetings being held on time and correctly minuted?
- Is there documentary evidence (via a SIP) that issues raised are being investigated and resolved?
- Are the SLA/OLA's current and what percentages are in need of review and update?
- What number or percentages of service targets are being met and what is the number and severity of service breaches?

2.1.9.6 Support Tool Requirements

To effectively support the Ideal Solution the service management tools within the Network Support and Supplier environments should be integrated. This integration can be achieved at various levels, ranging from the establishment of a central management information repository, to the introduction of a common Service Management platform across the multi-vendor environment.

POL00394097

The benefits of an integrated solution to the Network Banking service include: -

- A single source for all Service Management information
- Accurate measurement of both internal and supplier service levels
- End-to-End tracking of all incident, problem, change requests and known errors
- A central configuration management database (CMDB)
- More effective escalation processes
- More accurate change planning and scheduling
- Increased efficiency of all processes where multiple vendors would be involved
- More effective root cause analysis and trending within Problem Management

2.2 Definition of the Integration Options

A scoping exercise will be conducted to baseline the existing tools within the Network Banking environment and to establish the integration options available to the Post Office. This exercise will contain two stages:

2.2.1 Stage 1

Assess the suitability of the existing (and planned) tools within the Network Banking and supplier environments to support the ideal solution.

This study will focus on the following areas:

- The current effectiveness of the tool
- The available management information
- The scope of Service Management processes supported (Service Desk, Incident, Problem, Change, Configuration, Release, Availability, ITSC, Capacity, Service Level and Financial Management)
- The performance of the tool
- The scalability of the tool
- The underlying database architecture
- The format, validity and currency of the data
- Support arrangements (and planned development cycle for the system)
- Maintenance and version upgrade costs
- Available interfaces (both inbound and outbound) to other systems

Note: This study will draw on any tooling studies that have already been conducted within the Network Banking and supplier environments.

2.2.2 Stage 2

Define the options available to Post Offices for establishing an integrated Service Management system across the Network Banking End-to-End Service Management Model.

POL00394097

The options will be assessed against the following criteria:

- Indicative cost
- Indicative implementation time-scales
- Pros and cons of the solution
- Technical feasibility

Recommendations will be made for the option that most meets the requirements of the ideal solution.

POL00394097

3 Gap Analysis

Existing/Planned Roles and Responsibilities against Proposed Service Management Model

The following section identifies the ITIL processes as viewed at POL with their relative characteristics and current usage. Further conclusions and bottlenecks are indicated. Finally recommendations are made intended to focus the required work assisting POL in moving towards the ideal solutions as described above.

3.1 Configuration Management

3.1.1 ITIL Description

Configuration Management covers the processes of information management on IT assets. An unambiguous, reliable registration is of vital importance for the control over IT assets. The Configuration Management Database (CMDB) is used to register all IT items.

3.1.2 Introduction to Configuration Management

There is currently no single approved repository for the registration of IT assets or their interdependencies within POL. A number of disparate asset lists and in-house developed databases have been created containing different levels of detail relating to IT and business-focussed systems and processes. Technical Configuration Management (i.e. the recording of IT related equipment) is considered the responsibility of POL's major 3rd party supplier Fujitsu Services and Business Systems (BS); however there is some degree of record keeping done within POL when tracking the movement of Horizon kit, or any other equipment within the branches.

Configuration Management within POL (in particular Network Support – NS) relates, in the main, to the management of Products and Services, not technical equipment or infrastructure. The most comprehensive Configuration Management database was seen within Network Support and held information on the following products / services and their interdependencies:

- Products
- Tariffs
- Contractual Documents
- Outlets / buildings
- Items / equipment
- Manuals / reference
- Roles
- People
- Functions / groups
- Processes
- Data sets / applications

POL00394097

It is within this database that feed-ins occur from other areas concerned with equipment (though not necessarily IT equipment) and technical data. For example a weekly .mdb (access database) file is received from the Reference data team (from the Reference Data System – RDS) detailing any changes to baseline information relating to product/outlet attributes and relationships. It is not known how often, if at all, these systems are cross-referenced and the information held validated.

It is the Configuration Management team's responsibility within NS to maintain the information held within this database and there are some clear inputs to the system. I.e.:

- Harvester (Visual Basic) file containing new CIs & relationships
- Weekly .mdb file from the Reference Data team detailing product/outlet information
- Weekly file from Customer Management identifying access rights / toolset licensing baseline information
- Weekly .xls files from Network Reinvention project managers identifying changes to outlet/project baselines
- Monthly .xls file from Horizon BAU Manager detailing any Horizon related changes (these require manual input to the system)

Where any data does not fall into these clear input categories it is not clear by which means the information is discovered and hence input to the database. Likewise it is not clear that there are sound change management processes supporting the maintenance of the information, the production of management reports or the regularity of audits. Should this be the case it is a key candidate for consideration by POL and their requirements from TSD once Network Banking comes into play with the addition of a considerably more complex technical environment in which to operate.

If the NS CMDB is deemed to be the hub of the Products and Services Configuration Management process for POL (as it seems to be) it is also necessary to make this database available to the rest of POL organisation for any significant strategic benefit to be realised.

It is also important to communicate the associated Change Management processes and access methods to the database more widely.

Current usage

The existing version of the NS CMDB is used to:

- manage changes to the information held on the Network Business Support Centre (NBSC) knowledge base
- Identify and record the movement of Horizon kit within POL branches.
- Identify the total numbers of Horizon kit deployed in the network at a given point in time which in turn supports the management of POL's contractual obligations.

POL00394097

- Manage delivery of the Network Re-invention programme and enable the provision of key management information.
- Assist in the sequencing of change activity across the network to minimise disruption to customers, sub postmasters and employees.
- Identify problems associated with specific CIs, e.g. products, branches etc.
- Record and identify the relationships between business continuity plans and their impact on the automated environment.

Identification of IT assets

As previously stated, the management of IT assets is mostly outsourced either to Fujitsu Services or Business Systems. In the new Network Banking environment it will be the responsibility of the TSD to obtain such information from relevant 3rd parties and to amalgamate this in order to provide POL with an overall view of their IT and branch network infrastructure.

Management and verification

Due to the 'outsourced' nature of IT Configuration Management the management and verification of IT assets is currently carried out by Business Systems and Fujitsu Services, although POL does keep track of all Horizon and other equipment held on-site in branches. Again, in the new environment it will be the responsibility of the 3rd party suppliers and the TSD to ensure regular IT equipment audits are carried out and any areas of concern are highlighted and communicated to POL.

3.1.3 Conclusions

a) A simple MS Access database exists to register CI's (products, services and some Horizon equipment, but no IT assets) within NS
b) The NS CMDB seems to be a part of some POL Change Management processes but not all, and there is no evidence of documented Change Management processes directly relating to the upkeep of the information of the database in general.
c) Configuration Management function currently exists in a limited form – full Configuration Management has not been committed to with POL and it is not IT focused
d) Reports do not exist but there is the capability if KPI's were to be introduced
e) There is little evidence to show that other Service Management processes use the CMDB.
f) The CMDB is on a standalone tool (Access) that is not supported by organisation.
g) There are links to some key tools but is not integrated with Remedy – the main Service Management toolset
h) Identification of CI's and its Base Level is understood within NS Configuration Management only

POL00394097

i) No verification audits are carried out
j) Change impact assessments are carried out by silos without use of the CMDB

3.1.4 Recommendations

a) POL would benefit greatly from the outsourcing of the technical Configuration Management function, enabling them to concentrate on their core business, whilst still being provided with the necessary overall picture of the technical infrastructure that Network Banking presents. This overall view will enable POL to make sound Service Management decisions with better control and understanding of the IT Infrastructure.
b) The outsourced Configuration Management function should manage a centralised CMDB using an appropriate support tool – to be agreed between TSD and POL.
c) A Configuration Manager role should exist within the TSD. The role & responsibilities should be clearly defined between POL and the 3rd party supplying the TSD, with interfaces and expected reporting requirements agreed and understood by both parties. This process should be reflected in the Quality System and any Contracts.
d) The Configuration Management data (however supported) should enable the (technical) Configuration Items to be at a level which link to other items and be accessible to many support areas. A decision needs to be made as to whether technical Configuration data (which must be available to the TSD and other Service Management disciplines such as Change Management) will be amalgamated with the existing 'Service Configuration Data' that is held in the NS database. If the information is not integrated into one support tool serious consideration must be given as to the management of Changes within each of these separate databases and the integrity of the information upon which Service Management (such as Change & Availability) decisions are based, and from which management reports are extracted.
e) The right to update information should be rigorously restricted to authorised people. Changes to the repository should be logged, for quality and management reporting purposes.
f) Identification of CIs and the Base Level need to be clear and carried out by TSD and the following questions must be answered:
    - What information on the IT infrastructure is needed to be able manage the IT services efficiently and effectively
    - What information is needed for reporting purposes;
    - What information does POL and TSD expect to need in the future;
    - Which tool can support our decisions
g) Once established, the repository should be capable of producing reports relating to the status of Configuration Items e.g. items on order, installed, under repair etc.
h) There is a need for a verification/validation process. Staff and management need to be able to trust the information and there needs to be formal processes in place to ensure that information submitted by 3rd party suppliers is timely and accurate. If verification reports that the data

POL00394097

is not accurate, measures should be taken to improve the process. This should be the responsibility of the TSD Configuration Manager.

i) Ownership of IT assets must be clearly established.

j) Status accounting is an essential part of Configuration Management. The historical data on status should always be accessible for analysis purposes. This will allow for analysis of weak components or maintenance, etc.

3.2 Service Desk / Incident Management

3.2.1 ITIL Description

The Service Desk is the single point of contact for end users. The Service Desk deals with complaints from end users, provides support for the use of business procedures by end users and provides end users with information on the business service provision. The Service Desk acts as an intermediary between the business service organisation and the end user. The implementation of the Service Desk in an organisation should be such that: -

- Every end-user has one contact point, **their** Service Desk, within the Network Banking Support Centre organisation regarding questions and queries, advice and any NBSC Service disruption or requirement.
- All contacts between the end-user and the NBSC service provider should be via their Service Desk.
- The Service Desk provides prime information concerning incidents to other designated IT functions.
- The Service Desk should always represent the interests of the end-users within the IT organisation.
- The Service Desk owns all incidents on behalf of the business and is responsible for closing all incidents, but not necessarily responsible for fixing them.

3.2.2 Introduction to Service Desk

POL operates two distinct Service Desks situated at Dearne House, Barnsley. The first Service Desk is Post Office External (POEx) which is an internally outsourced desk by Consignia Customer Management (CCM). POEx is a one-stop desk for use by the general public to enquire about Post Office related issues. For the focus of this report a concentration will be made on the second desk operated by NBSC. The assumption is that any technical difficulties experienced by the public in relation to the Card Account Programme (CAP), Network Banking or Electric Funds Transfer at Point of Sale (EFTPos) will be reported directly to a postmaster or a sub-postmaster at point of failure.

This report recognises that there will be an increase of calls to POEx, but it is the NBSC, which will be, impacted the most by the new projects.

The NBSC operates a Single Point of Contact for POL Counter Services (POCL). It supplies an Interactive Voice Response (IVR) system with three options to divert callers to the correct support area.

POL00394097

The first option is the "Incident Management Team" which is responsible for dealing with incidents, such as robberies of branches. This option is operated 24 hours a day. The core hours operated at Barnsley are 8 a.m. to 6 p.m., with all calls after the core hours are transferred automatically to a call centre at Oxford.

The second option is the Horizon System Helpdesk (HSH). This option is also operated 24 hours a day, with all calls transferred to the Fujitsu Services Helpdesk.

The third option is NSBC which operates 8 a.m. to 6 p.m. Monday to Friday except Wednesdays when the operational hours are 8 a.m. to 10 p.m., where the extra cover is for balancing issues at post offices. There is also a slightly reduced service on a Saturday 8 a.m. to 5.30 p.m.

The NBSC is made up of two levels of expertise, the first line is known as tier one and the second line team is referred to as tier two. Should third level expertise be needed for NBSC, second level will call upon the expertise directly from business units to aid in the incident resolution.

The NBSC also has several internal support groups:

- Incident Management
- Performance Implementation Advisors
- Capacity Management
- Projects & Training Team
- Customer Relations

Incident Management is responsible for monitoring real time trend analysis reports, which are located in a Lotus notes database.

Performance Implementation Advisors will communicate pro-actively with branches about process improvements.

Capacity Management function is responsible for ensuring that there is enough staff available per shift to maintain levels of service from the Service Desks.

Projects & Training function are responsible for staff training needs analysis and managing work undertaken to ensure when projects go live all appropriate documentation and changes in working practices are in place.

Customer Relations is a complaints department, handling complaints about the performance of NBSC or the HSH.

The software package used by the NBSC for recording and tracking incidents is Remedy. Currently, approximately 20,000 calls are recorded on Remedy each week, including all queries and incidents received.

POL00394097

3.2.2.1 1st-line support:

The Service Desk Advisors on tier one are responsible for taking all initial records passed through from the IVR. Tier one currently resolves 80%-85% of all incidents received, well over the 75% target. Tier one is also expected to collect and record on the Remedy system, sufficient data for Tier two to be able to continue to resolve an incident.

The two tiers both utilise the Kbase knowledge management system, which contains all procedures, including, work arounds. NBSC has a well-structured scripted greeting for the callers into the service. Although a unique number is automatically given to an incident record, it is not the practice of the NBSC to quote a reference number to the caller. All calls received are recorded by category and allocated a priority.

Calls are escalated to tier two should tier one not be able to solve the incident. Tier two resolve around 80% of all incidents passed to them initially. Any incidents that that need further investigation are done by tier two with the aid of business unit specialists.

Fujitsu Services logs all the incidents received by HSH on the incident recording system. The incident record does have a unique identifier that is communicated to the caller. Should the HSH desk be unable to resolve the incidents initially it will call back with a resolution to the incident originator or escalate the incident to problem management.

3.2.2.2 Interface between POL and Post Offices:

It is unlikely that the NBSC is being bypassed by POL counter staff going directly to business units for help in resolving their incidents.

The NBSC does not receive an IT Forward Schedule of Change (FSC) from change management detailing forth coming changes that have a potential impact to POL. The NBSC is used to communicate any changes in company Policy, Procedures to the Post Office branches.

The NBSC is only responsible for business process and procedure related calls though tier two has been resolving incidents relating to the Horizon system which should be resolved by the HSH.

3.2.2.3 Management reports:

The Incident Management team produces and monitors real time trend reports produced by Business Objects form the Remedy System. The following report is a sample of the trend reports available:

- Incidents reported by against each client.
- Incidents reported by against the Horizon System.

POL00394097

- Incidents reported by against categories per day.
- Incidents reported by against categories per hour.
- Incidents reported by against each branch.
- Incidents reported by against each region.
- Incidents reported by against postcodes.
- Incidents reported by against post town.

3.2.3 Conclusions

a) The current Service Desk will not be able to cope with technical incidents.
b) The demarcation of responsibilities between the tier two and HSH need to be resolved, as tier two is receiving and resolving Horizon related incidents, which is leading to a confusion of resolver group responsibility.
c) A review into why high volumes of calls are being transferred between HSH and NBSC (totalling approximately 3000 calls a month) is needed, as this problem may increase once the TSD has been put in the place.
d) The interface between the Service Desk and Change Management needs to be strengthened. As the main focal point for POCL end-users, when they have a problem, the Service Desk should have stronger representation at Change meetings. Without this, the ability of Service Desk management to plan effectively in advance, in relation to resource and training needs, is seriously affected. There is also a potential risk of being unprepared, where IT changes results in an increased number of calls. The level of pro-activity of the Service Desk in raising customers' awareness of pending IT related changes could also be improved.
e) There is a need to formalise the non-contractual agreement called the Interface Agreement, detailing how incidents are handled between NBSC and Fujitsu Services. All agreements between external and internal suppliers should be standardised formal agreements.
f) The Remedy tool set has been developed to deal with incidents relating to business process and Horizon system incidents. The future requirements of the system need to be identified and documented.
g) Better integration between the different incident management systems operated by the NBSC and its suppliers.
h) The distribution of the trend reports seems to be limited to within the NBSC Service Desk environment.

3.2.4 Recommendations

a) The implementation of a Technical Service Desk (TSD) to manage and take ownership of technical Incidents on behalf of POL. This desk will provide a skilled single point of contact for technical support requests.
b) With the implementation of the TSD it becomes increasing imperative to insure that resolving teams only take ownership of incidents that are defined within their scope. This will ensure that correct metrics for each delivered service are being produced, as well as ensuring that staffing levels for each service are set to the correct level.

POL00394097

c) A formal relationship with related Service Management processes needs to be established. The NBSC Service Desks should get involved at the awareness stage of an IT related change which has the potential to impact the POCL services and be involved in suitable change management meetings.
d) The one external supplier to POL Service Desks has an interface document detailing the relationship between the supplier and POL. The interface document needs to be ratified and produced in a standard SLA/OLA format.
e) A review should take place of the current effectiveness of the call logging software package. Terms of reference should be drawn up which would require the identification of all requirements, including the need to deal with integrated processes.
f) As part of the review listed in e), the review should also look at the different options available to either implement a single tool across the different suppliers or find a technical solution to allow integration between the different tool sets.
g) To ensure the most productive utilisation of these reports a promotion and wider distribution of the trend reports is necessary. Trend data is an essential part of the problem management process; therefore a review is necessary to ensure the trend data needed by Problem Management needs to be undertaken.

3.3 Problem Management

3.3.1 ITIL Description

Problem Management is a discipline that deals with the processes of identifying, diagnosing and solving problems and preventing disruption to the supplied services.

The main concepts and definitions within Problem Management are:

- An **incident** which is an operational event, which is not part of the standard operation of a system. It will have an impact on the system, although it might be slight and may even be transparent to users
- A **problem** which is a condition identified from multiple incidents exhibiting common symptoms, or from a single significant incident, indicative of a single error for which the cause is unknown
- A **known error** which is a condition identified by successful diagnosis of the root cause of a problem, when it is confirmed that a Configuration Item is at fault

3.3.2 Introduction to Problem Management

The Problem Management function is situated at the Dearne House, Barnsley site. Problem Management is part of NS operated by the POL.

POL00394097

The Problem Management team reports to the Service Quality Manager and is comprised of five Problem Managers with six Problem Analysts reporting into those Problem Managers. The other teams within the group are Business Continuity Management (BCM, five analysts), Process Efficiency (PE, three analysts) and the Configuration Management (CM, two analysts) . The core hours of operation for the Problem Management team are between 9:00 a.m. and 5.00 p.m.

The Problem Management function is proposing a restructure of the team. The restructure would see the appointment of a Duty Manager from one of the current five Problem Managers. This role would require the Duty Manager to be on call 24 hours a day. The remaining four problem managers would report into the Duty Manager. The Problem Management team will also restructure to take into account the Network Banking project by allocating a dedicated Problem Manager for that service.

The types of Problems managed by the POL Problem Management team fall into two distinct types:

- Business process related problems.
- Horizon system related problems.

The current role of the Problem Management team is well documented and understood throughout the business organisation. The Problem Management team is responsible for the raising of problems on the Remedy system, tracking and monitoring the problem until resolution. Each problem raised is given a unique number for identification and reporting purposes.

The Process Efficiency (PE) team is also responsible for Problem Management. The PE team proactively identifies Post Office branches that need advice and guidance in utilisation of POL business procedures.

The current Problem Management procedures are well documented and include a high level process, a more detailed generic process and a major incident handling procedure.

The software package used to monitor the problems is Remedy. All temporary work-arounds identified and produced are stored in Kbase a POL Intranet solution, utilised predominantly by Tier one and Tier two.

3.3.2.1 Major Incident control:

The Problem Management team at POL have a well-documented procedure for the major incidents (i.e. an incident of significant impact that is escalated to a Problem). Members of the NBSC service desk escalate the major incidents to the Problem Management team, when it becomes apparent that there is a major incident or an abnormal number of calls being received by the Service Desk indicating a potential problem occurring in POL business operation.

The Problem Managers do not manage the major incident; instead the BCM team members manage it. They will check the incoming data and check the data

POL00394097

against decision trees located in the Major Business Continuity Incident (MBCI) Trigger Guide. Once the major incident has been accepted as a MBCI it is owned by the BCM team or if the major incident is deemed not to be an MBCI the ownership for resolution will be reverted back to Incident Management within the Service Desk function.

After the successful resolution of the MBCI a Post Incident Review (PIR) will be carried out to determine any further actions that would safeguard the business services in the future.

The Problem Management team interfaces Fujitsu Services who are responsible for the Horizon System. The relationship between the POL Problem Management team and Fujitsu Services is documented in the Interface Agreement Document detailing the procedures for major incident handling.

During a major incident involving Fujitsu Services a duty manager from the supplier acts a central point of contact for the Problem Management team. The duty managers co-ordinates the work being undertaken by Fujitsu Services staff, whilst the POL Problem Managers communicate to the business via the Crisis Management team. The Crisis Management team is made up of senior business managers within POL.

3.3.2.2 Problem / error control:

Problem Management investigates all incidents that are progressed by the Incident Management function located in the NBSC. Once recorded in the Remedy System the Problem is passed to Problem co-ordinators. The Problem co-ordinators are nominated experts in their business units. They will ensure that a problem is progressed in their area and an appropriate solution is delivered. This solution will take the form of a temporary procedure (TP) or an agreed temporary procedure (ATP). Problem Managers will ensure the problem is being progressed, due to, the Remedy system keeping the Problem Record in the work queue of the Problem Manager.

Incidents that have progressed to Problem or MBCI are not easily linked to a change. It is difficult to see changes done to the POL IT environment and Horizon environment, as there is no published Forward Schedule of Change (FSC).
There are distinctions made between Incidents, Problems and Known errors on the Remedy system. Categorisation happens in an Incident Record; categorisation is not done within a Problem Record.

The Problem co-ordinators have access to the Remedy system, and are able to update the Problem Records assigned to their business unit. The Problem Managers monitor the quality of information within the Problem Records.

Known errors are progressed into the Kbase knowledge management system. Here all the TPs and ATPs are accessed by tier one and tier two. ATP's can be quickly accessed and work arounds conveyed to the business users. Kbase is only used for IT related issues stemming from the Horizon system.

POL00394097

3.3.2.3 Proactive Problem Management:

One of the main purposes of the Problem Management function is to insure a proactive approach to dealing with business issues. To this end Problem Management undertakes Root Cause Analysis (RCA) either from trends identified by the Incident Management function at the NBSC or after a MBCI. Currently, Problem Management concentrates mainly on MBCIs.

Trending on incident information is undertaken by interrogating and analysing Remedy records via Business Objects. However, it is a team called 'Incident Management Team' within the NSBC that is responsible for producing and initially investigating emerging trends. The flow of information generated by the Business Objects reports needs to be distributed to the Problem Management teams.

3.3.2.4 Management reports:

The Problem Management monthly report includes a management summary of the previous month highlighting key problems and issues faced. The report also lists all problems opened up during that months reporting period and a section on outstanding problems older than 3 months.

The report also includes the number of open problems remaining and groups these by the total number of days outstanding. The report also shows a breakdown of problems owned by the business units, with a further section dedicated to the amount of problems affecting each POL service.

Problem Management performance metrics also form a section in the monthly report. Within the performance section there is an activity dedicated to quality assurance of information recorded in the Problem Records.

3.3.3 Conclusions

a) Problem Management currently monitors, tracks business process related problems and Horizon system problems.
b) The service levels that have been set for problem and incident handling need to be realistic and in harmony with other dependencies.
c) The Problem Management process and procedures whilst being well-documented need to be reviewed for consistency and relevance.
d) The adequacy of the software package in relation to the new service, needs review
e) A review of the Performance Implementation Advisors function and the Process Efficiency analysts further needs to undertaken.
f) A review into how problems are escalated and prioritised.
g) Root Cause Analysis needs to be applied to all incidents to ensure that trends are being identified and underlying issues dealt with.
h) Stronger links between Problem Management and Change Management need to be built and understood.
i) A review of Problem Management supplier meeting needs to be undertaken.

POL00394097

j) A review of the working relationship between the Service Desk/Incident Management and Problem Management.
k) There is a need for harmonisation of operational working hours between the Service Desks/Incident Management and Problem Management.
l) The creation of a more comprehensive configuration management database would greatly enhance the effectiveness of problem impact analysis.

3.3.4 Recommendations

The role of Problem Management needs to be expanded to the following areas:

Future IT suppliers to POL
Internal IT suppliers to POL

As the IT infrastructure needed to deliver the services of POL expand due to the Network Banking Project, the diversity and complexity of the interrelationships between IT infrastructure components and their related business process will increase. In order for Problem Management to truly manage the problems created from Network Banking Service it must be able to affect all components listed for an end-to-end service provision. Problem Management must be able to effectively interface with all suppliers both external and internal to insure that co-operation across different expertise domains is progressing problems identified, which are affecting the business adversely.

b) All service levels should be reviewed and standardised into a format which can be rolled out to all existing suppliers to POL both internally and externally, with a view to ensuring all new suppliers providing services to POL conform to the same standards.
c) The one external supplier to POL Problem Management has an interface document detailing the relationship between the supplier and POL. The interface document needs to be ratified and produced in a standard SLA/OLA format.
d) POL has undergone rapid change's over the last 12 months, it is essential that all documentation related to Problem Management be reviewed and updated with all the new name changes to reflect the current organisation.
e) Problem Records on the Remedy System use mainly free text fields, there is currently no categorisation pick lists to open a problem record or on closing a problem record. With a view to improving the Problem Management function and with the potential increased needs for the expanding POL service provision in Network Banking, a review of how Problems are categorised need to be taken.
f) The PIA analyst role and the PE analyst role should be combined to produce one team that will effectively advise and mentor branches on operating procedures. It would also ensure single ownership of improvements to be communicated to the branches, instead of one team having to inform another team of what needs to be communicated to the branches; this would provide a more efficient process.

POL00394097

g) Currently the way in which problems are prioritised is working well. The Network Banking project and the possible expansion of the Problem Management function would mean a speedy way of prioritisation of more varied Problems will need to be made. The speed of the current system for prioritising Problems would possibly limit the effectiveness of the future development of the Problem Management function.
h) The NBSC Incident Management team does produce trend reports on incidents recorded in Remedy. Clear lines of demarcation of roles and responsibilities need to be agreed between the Incident Management team and the Problem Management team, detailing how trend reporting and progression is accomplished. This review into roles and responsibilities should be done at the same time as the review outlined in recommendation f).
i) With the advent of the proposed Technical Service Desk a need to produce a requirements document for how trend information will be reported on and passed to the POL Problem Management team needs to be undertaken.
j) The Problem Management team does not have sight of a FSC detailing all the planned changes to the IT Infrastructure of POL. A review of how changes are communicated to Problem Management needs to take place.
k) Problem Management has an established monthly meeting with Fujitsu Services to discuss problems and issues. Problem Management would need to increase the scope and attendees of the meeting by having all suppliers attend. The suppliers would be from both internal and external to POL. This will ensure that cross platform issues are expedited efficiently and effectively.
l) The current ownership of the meeting is shared between Fujitsu Services and Problem Management. The future meeting would be a forum chaired by the Problem Management team to ensure consistency.
m) A review on how incidents are escalated to problem management needs to take place, as there is a perception that Problem Management may need earlier warnings of incidents with the potential to cause a significant impact to the business. As part of the Remedy review the requirement for automatic alerting to certain categories of incident into the Problem Management area may be considered.
n) A synchronisation of working hours between Service Desks and Problem Management will ensure that disparity between operating times no longer exists, with Problem Management being able to respond to all incidents that need to be escalated. This will become more critical as the services offered to the branches increase with real time banking.

3.4 Change & Release Management

3.4.1 ITIL Description

Change Management provides a mechanism to manage the initiation, implementation and evaluation of changes in the operational IT organisation. Controlled implementation of changes is vital for a reliable and flexible IT service. Change Management is a generic process that covers the IT infrastructure

POL00394097

(hardware, software, and documentation), the IT services (SLAs, service characteristics) and the IT service organisation (structure, procedures).

Release Management comprises activities concerning planning and overseeing the successful rollout of software and related hardware and to ensure that hardware and software being changed is traceable, secure and that only correct, authorised and tested versions are installed. Further, it covers the management and distribution of operational software that must restrict the risks of unauthorised use, unauthorised change and destruction.

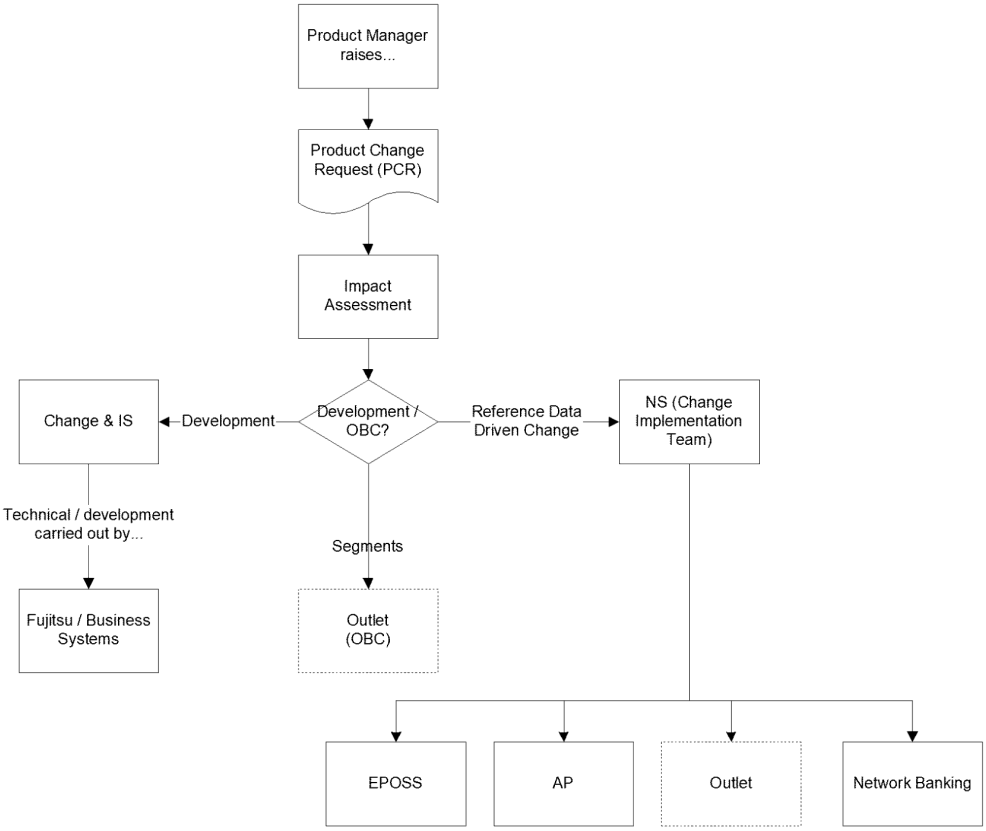
3.4.2 Introduction to Change & Release Management

Change in POL consists of two key areas managing Change Deployment and Service Development and there are two key roles responsible for the provision, and management, of effective change. They are:

- Network Change Control Team (belonging to the Operations Directorate and are part of NS);
- Infrastructure Programme Integration Team (part of Change and IS Directorate Change Control) dealing with Company Wide Change Initiatives

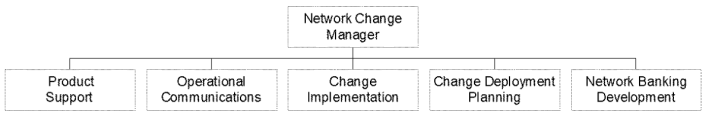
The first of the two groups is responsible for day-to-day data driven and ad-hoc changes and / or those that come under the PACE Change Control Process (described in more detail below) and is headed up by Nick Embling. The latter deals with any changes resulting in New and Changed capability within POL services and is headed up by John Bruce. The diagram below illustrates the split:

POL00394097



PACE (Progressing & Achieving Change Effectively) is an accelerated Change Process for 'standard' Product Changes. It is the responsibility of Beverley Dunn's teams in the Change and IS Directorate and is a process which seems well understood and adhered to throughout POL. If a product is present on the PACE selection list then it can enter the accelerated Change Process, encouraging best practice by minimising unnecessary bureaucracy and "red tape". In terms of best practice Change Management this is one of the most effective ways of encouraging adherence to the process by those involved in Changes and is an efficient and cost effective way to manage standard changes from a business perspective.

Within Nick Embling's Network Change group there are a number of sub-groups:



POL00394097

The Change Implementation Team based at Farnborough manage all Reference data driven changes including automated payments and EPOSS changes (a manual version of AP) and is managed by Rabia Cody. The actual changes are made by Fujitsu Services, but are tested for acceptance by (Operational Business Change) OBC, part of the Change Implementation Team. This team will also be involved in managing the day-to-day reference data driven changes within the new Network Banking environment.

OBC have 2 clear documented change processes detailing the lifecycle of changes in the following areas:

- Products
- Network (of branches)

The scope of the OBC function is to be extended to include similar affecting changes in the new Network Banking environment and it is the responsibility of OBC within NS to develop the processes in time to incorporate Network Banking.

Currently Reference Data is stored in the POL Reference Data System (RDS), owned by Business Systems but NS are responsible for data input to the system. This contains version controlled release and network (branch) information which is replicated with Fujitsu Service's equivalent system (RDMC). There is more information held on the Fujitsu Services RDMC database than POL's and future access to some of this extra information has been mentioned as something that would be useful to POL. Some of the information relating to the branch networks within POL RDS is also duplicated within the NS CMDB.

A 'reference data model' exists which has been expanded to incorporate Network Banking requirements and it is understood within OBC that the current interface agreements between themselves and Fujitsu Services with regard to Change Type Catalogues and associated lead times will need to be replicated with the new suppliers that Network Banking brings.

The Change Implementation Team test any product changes (reference data driven) and are responsible for authorising the change to be released into the live environment. The process is clear and documented and seems to work well, though there are sometimes problems with the communication of changes generated from other parts of the business. Indeed the Change Implementation team are made aware of some changes for the first time when they are contacted by Fujitsu Services requesting "live release" authorisation.

The team have their own Change Management Database, built in-house on Access, which is only shared within this team and it is said to be fairly unstable. The OBC team are looking for an alternative solution to support their work.

By mid May 2002 Change Management will be responsible for the management of ALL aspects of the Operation Directorate changes. This is due to the merger of the Change Control and Change Deployment teams (currently separate). These teams are being combined in order to provide a holistic view of the impact of any changes enabling the assessment of all changes not only from a technical

POL00394097

perspective but also taking into consideration the "personnel" and branch capacity issues.

The team will be made up of 10/12 people receiving Product Change Requests (PCRs) from the business as a first official point of contact which, in turn, will trigger an impact assessment to be carried out.

The Change Control team is currently split into 2 segments:

- Product Support, who are based at Gaverelle House and are responsible for actioning day-to-day improvements to products &

- Development Co-ordinators based at Prospero House who look at and support major business changes and the major change program published by Change & IS Directorate. They also co-ordinate all NS changes. Request inputs to this team are mainly from Change & IS and / or Strategic Alliance Directorate either direct or through Business Architecture (BA).

The Change Deployment Team will continue to act as the Operations Change Communications team. They are based at Gavarelle House and are responsible for the production of manuals and instructions of new processes, and "Counter News" – a weekly newsletter distributed to all branches.

Change and IS Directorate is responsible for the Change process as a whole across POL. They are the owners of the Business Change Plan and look at the changes which have been scheduled ensuring strategic alignment. The Business Architecture group (headed up by Sue Harding) is also responsible for checking each major change for strategic alignment and have a 10 box model against which changes are compared to ensure all areas affected by the change are considered before approval. Key interfaces with Change and IS are OBC – responsible for managing physical changes in outlets and Business Systems (BS) – those responsible for on-site POL technical support. They also produce the Business Release Plan.

There is also a Change Control Board consisting of representation from both POL and ICL Pathway and there are representatives from the Infrastructure Programme Office (headed up by John Bruce) who sit on this Board. The Infrastructure Programme Office is part of Change and IS and manages the Change Plan, Release Plan and is responsible for the integration of change across POL. The documented processes used by this team detail the basic operation of change control for the Change & IS area, in particular the Horizon system operated by Fujitsu Services. They also cover the back end systems that provide accounting / management information for POL, supported by Business Systems (BS).

Overall Change & IS Infrastructure Change Control are responsible for:

- validating a change request and ensuring that it is complete and that its intention can be clearly understood

POL00394097

- registering a change request on the Programme change database (another separate database, not widely used within POL and certainly not available across directorates)
- identifying what dependencies there are from a change and what areas within or external to the Programme are likely to be affected by it
- deciding with the originator / business owner who should be involved in the impact assessment
- determining the length of the assessment period
- issuing a change request (CR) to impact assessors and ensuring that they respond in due time
- confirming where the responsibilities for funding and authorising the change are and that budgetary provision has been made and approved

There is an in-house built database which belongs to the Infrastructure Programme Office which holds information pertaining to Horizon System Changes. This database is exclusively available to this team to assist in the management of their work and is built using Access 2.0. The team are looking to move it to a Lotus Notes platform.

To summarise into ITIL best practice elements, POL performs the following:

3.4.2.1 Acceptance/registration of changes:

In most cases there are clear, unambiguous and well documented processes by which the relevant teams are made aware of the need for Change. However, there is not a single point of entry for the registration of changes, nor a single repository containing detail of ALL changes.

3.4.2.2 Planning and Control of changes:

As previously mentioned it is the Change & IS Directorate who manage and own the Change and Release Plans for all of POL, but there does not seem to be a clear link into these documents from NS and any changes they may generate, perhaps as part of their 3rd line support role. There seems to be sound planning and control of changes within the individual 'change involved' directorates, but a lack of co-ordination between the two.

3.4.2.3 Check on the execution:

It is clear that Change Management within both Change and IS and Operations Directorates 'keep tabs' on the entire change process when a change is their responsibility. It is not clear however (as the individual supporting databases were not viewed) how change progress is documented or registered – and consequently reported on.

3.4.2.4 Evaluation of changes:

The Horizon Change Request Form is a standard template used by the Horizon Change "involved" teams. It contains detail of the Change requestor, the purpose, impact and description of the change (including the impact of not implementing), the urgency and costs. However it does not seem to have a "review" section so it is not clear whether changes are reviewed within POL at all, whether successful or not.

POL00394097

There is also no single standard reporting function nor single repository for the information relating to Change Management across POL, so it is unclear how changes and the effectiveness of the overall function is evaluated.

Software Storage:
ITIL best practice states that those parties responsible for 'Software Management' should ensure that reliable copies of software items are available to the organisation and that copies of the correct version are used for development. This is very much managed by Business Systems (BS) and Fujitsu Services who look after the technical aspects of POL support, owning the RDS and RSDC Definitive Software Libraries (DSL's) respectively.

Release construction:
A release schedule does exist within POL and there is an allocated Release Manager responsible for the creation of this schedule and integration and communication of it to POL, BS and Fujitsu Services.

Software Distribution & Implementation:
Again, the distribution and implementation of software or any changes to software is actioned mainly by Fujitsu Services at this time within POL. However there are clear processes, contractual agreements and the understanding between the 3rd party supplier and POL which mean that POL test any changes and authorise before any releases into the live environment.

3.4.3 Conclusions

There is clearly the capability to manage all aspects of change and release within POL. Indeed the technical, strategic, business facing, people and training issues have all been addressed within one or more areas of the change management teams across POL. However, there seems to be a lack of communication, co-ordination and single repository for information within POL, particularly between directorates which may cause some concern when the operating environment becomes more complex.

Change within POL is severely distributed both procedurally and geographically with no single support tool, or overall picture of change showing a full understanding of where all "change involved" teams interface within the organisation, their roles and responsibilities. Each team seems to have built their own change management database to assist them in their day-to-day administrative tasks, however, these are often on unsupported / non-standard software products (i.e. Access 2.0) and do not enable POL to gauge an overall view of all technical and business changes at any one time. Where change processes do exist and work well, they are not always documented or communicated well.

In summary:

a) There are elements of Change in many pockets throughout NS and POL, but these are not centralised in any way and do not share any common tool.

POL00394097

b) 3rd parties manage elements of the Change process themselves and it is unclear how well this communication process works back to NS. The lack of documentation places POL at risk and does not make it easy to replicate 'good' change management processes with new suppliers (i.e. those introduced through Network Banking) or advertise the effectiveness of those processes well within POL.
c) There is a lack of ability to derive impact assessment data due to a lack of strategic configuration management database (CMDB)
d) No commonality of function at a group level. Despite the Change & IS Directorate being responsible for overall Change within POL and having a clear understanding of how the function should work there seems to be a fundamental lack of understanding of roles between Change & IS and Operations. This may simply be due to a lack of effective communication or co-ordination between Change & IS and Operations Directorates, or may require some re-engineering of process or more senior management input and attention.
e) There is no clear evidence of Change Advisory Board other than the Change Control Board which exists between the Infrastructure Programme Implementation Team and Fujitsu Services. There is not one CAB however which examines, co-ordinates, authorises and helps to schedule ALL changes across Change and IS and Operations.
f) There is no clear view on where or how business criticality levels are derived Despite there being some well understood and implemented processes within POL and between 3rd party suppliers it is not obvious that these are documented and therefore able to be replicated with future suppliers or easily followed by new employees.
g) There is no evidence that evaluation of changes take place.
h) Product changes follow an unambiguous test, authorisation and release pathway, demonstrating sound understanding and application of the software distribution elements of ITIL best practice Release Management.
i) There is a single DSL (BS RDS) which is mirrored, in the main, with Fujitsu Services' RDMS
j) The DSL and DHS are managed by Business Systems

3.4.4 Recommendations

a) Change Management should be centrally implemented and controlled within the Change and IS Directorate. This function must then be documented and well communicated to POL perhaps through workshops or presentations due to the importance of adherence to the overall Change Management function and the need to express the challenges presented by the introduction of Network Banking and the purpose of the function. However, Network Support should maintain final approval for releasing change into the Network Banking environment.
b) A fully ITIL compliant Change Advisory Board (CAB) should be implemented
c) There should be a central unambiguous registration of ALL changes for POL
d) Categorisation, planning and priority setting should be controlled via a central location
e) Scheduling related to capacity & resource schedules should be produced and distributed to the appropriate resources within POL as part if the Change Management Process

POL00394097

f) Investment should be made in a Forward Schedule of Change tool to more easily facilitate the production of this report showing ALL changes for POL
g) Standard KPI's should be defined and agreed to measure the quality of Change Management.
h) The definitions of change, when the change processes should be activated, the definition of change categories: standard change, emergency change, minor impact, medium impact, and major impact, should be documented at an overall POL level and well communicated to advertise the scope and understanding of Change within POL to internal staff, gaining commitment to the processes.
i) Attention should be paid to the scheduling of changes and a Forward Schedule of Change and 'Projected Service Availability' (PSA) should be produced for ALL changes. These should be accessible to all within POL via the Knowledge Base perhaps.
j) A standardised Change Request Form possibly based on the Horizon Change Request Form but preferably electronic and part of an integrated Service Management tool, will greatly benefit the company wide change process. All parties involved in changes should have input into which fields of the form are required (such as Impact, Category, authorisation, business case), and which fields are facultative (e.g. preferred date of implementation). With electronic forms, registration is facilitated. Each change should be recorded in a central repository, to which the different support groups should have at least read rights. The TSD and NBSC should be informed of each emergency change. Communication pathways must be clear to ensure this information transfer.
k) Change logs should be updated with each step of Change Management activity, from authorisation, to build and test, to implementation and review.
l) Communication of changes is crucial. The TSD and NBSC should be made aware of all scheduled changes. The business should be aware of scheduled changes where there may be a business impact, for example an outage. Support staff should have access to the Change Management database to assist in speedy problem resolution. It is essential that incidents can be linked to changes. Changes that are in one way or another visible to end-users should be communicated through the NBSC in collaboration with the appropriate communications team within POL, in order to keep the single point of contact for end-users.
m) Third parties should introduce each change they perform through the POL Change Process either directly or via a nominated internal party (TSD perhaps).
n) Document Management should continue to be part of the Change Management process and be supported by the common support tool.
o) Support teams should be involved at a consistent point in the project lifecycle to enable their inputs to be taken into account and to allow them to adequately prepare to test, manage the implementation of, and support new services.
p) With the expected step change in the provision of services due to Network Banking the number and complexity of changes will increase many-fold. Overall control of change must be instigated, and communications improved between the two key change groups in Change & IS and Operations.
q) Change, Release and Configuration Management must be inextricably linked.

POL00394097

r) All required information assisting POL in the effective management of change should be obtained from Fujitsu Services' RDMS. This must then be fully duplicated in BS' RDS and subsequently in POL's CMDB

3.5 Availability Management

3.5.1 ITIL Description

Availability Management assures the optimisation of availability and reliability of the IT infrastructure and supporting organisations providing IT services. Availability Management systematically optimises preventive, inspective and corrective maintenance of IT service processes. In addition to technical aspects, organisational, procedural and security aspects play an important role.

3.5.2 Introduction to Availability Management

Within POL there is no single function responsible for planning and monitoring end to end availability across all platforms. Consequently, no interviewees were made available to PinkRoccade during the production of this report.

Availability targets are in place, or are currently in negotiation, for the availability of the systems within the end to end Network Banking environment. These relate to individual platforms and not for the end to end service. The design of the Network Banking environment has incorporated a number of measures across all platforms to reduce the risk of downtime experienced by the end users.

Designing and Planning for Availability:
Evidence was found of attention being given to the issues of reliability and availability within the technical solutions designed for the Post Office.

3.5.3 Conclusions

a) Some aspects of Availability Management are carried out within other functions e.g. Problem Management. However the full range of responsibilities of Availability Management are not all covered across all platforms and should be assigned. The range would include:-
    - Drawing up plans to ensure that long term serviceability objectives are met.
    - Working alongside development teams so that project requirements for availability are feasible and accurate and result in relevant supporting obligations by suppliers and other areas of the Post Office, enabling the finished product to run smoothly in production, with no surprises.
    - Initiating changes to ensure that availability of services is improved in a cost-effective way.
    - Questioning, collecting and registering customer demands regarding availability, in line with service levels.

POL00394097

- Analysing all of the Service Areas' infrastructure components and those of other service delivery areas, so that factual availability information can be collected. Configuration Management would assist with this.
- Registering measurements regarding availability i.e. monitoring and reporting on availability of services and their components compared to service level agreements.

b) As an adjunct to the above, there is no single point of ownership of Availability Management.
c) Availability targets are currently not formally agreed with the business and are focussed on platform specific targets and not the end to end service that the customer receives.
d) The performance of third party equipment is not being monitored consistently. Performance issues are only raised with suppliers when the contracted service levels relating to incident and problem fix times have been breached.

3.5.4 Recommendations

a) The function of Availability Manager should be assigned to someone within the Network Support area, who should be asked to define the role and responsibilities and draw up an action plan for its adoption. This could form part of an existing role e.g. Capacity Management or SLM
b) Availability data should be formally discussed in order to agree on targets, which match the requirements against the suppliers' ability to deliver them. These targets should reflect end-to-end availability and should then form part of a Service Level Agreement.
c) A virtual Availability team consisting of representatives from each area of the E2E environment should be established. A BI-monthly meeting should be held and used as a forum for the discussion of capacity matters.
d) The focus of Availability targets should be reviewed and consideration given to broadening the scope to include an end to end view of service availability.
e) Before committing to targets for achievement with the branches, the suppliers need to be inline with these numbers and signed up to them. If targets required by the business cannot be negotiated with the suppliers, due to reasons such as high maintenance and support costs the business must be informed of the implications to overall availability targets.
f) It is important that each incident is recorded, as this will form the basis of outage data. The actual unavailability experienced should be confirmed with the customer at the time the incident is closed. This should ensure that not only is the unavailability data recorded, but will avoid any disagreements at a later date. Concentration can then be on the service implications of the outage and any preventive action that might be taken etc. Setting a downtime flag on the incident recording software (Remedy) should enable such data collection to be less time consuming.
g) Appropriate tools should be investigated and implemented to aid the measurement of end to end component availability. This information should then been used during supplier meeting when discussing performance and reliability of supplied hardware and software. Where

POL00394097

possible suppliers should be expected to supply accurate availability information at service reviews.

h) Responsibility for collating and issuing reports to the business relating to all aspects of service provision should be coordinated from a central function. This is typically the service level management function.

i) Monitoring of third party supplier performance with regards to their ability to meet availability and fix time targets should be routinely performed and not only when an exception occurs. Creating a field within the Remedy tool to reflect an assignment to a third party, would enable tracking and reporting on performance to become less time consuming.

3.6 Capacity Management

3.6.1 ITIL Description

Capacity Management assures that the correct capacity is available at the right time in the right place at justifiable cost. Capacity Management has an operational task in ensuring that continued daily business use of IT can be supported with the currently available IT resources. Capacity Management has task at a tactical level, which entails the expansion or shedding of IT resources, in order to match business needs. The amount of data that needs to be processed and the associated performance requirements should be reflected in the Service Level Agreement

3.6.2 Introduction to Capacity Management

Within POL the Capacity Management process is fragmented across the business, with no single function being responsible for planning and monitoring end to end capacity across all areas. Capacity is mainly viewed in terms of business processes with the technical capacity being managed within each platform area.

3.6.2.1 Capacity Planning:

Capacity planning is conducted but is fragmented across the various areas of the business. No evidence was found of a centralised Capacity plan or Capacity Strategy that focuses on the end-to-end environment.

3.6.2.2 Capacity Database Creation:

A central Capacity dB does not exist within the Post Office. The Capacity interviews uncovered various capacity models being maintained within different areas of the business, focusing on: -

- The planned impact of Network Banking on the NBSC and POEx Service Desks. This model calculates the additional call volumes that will be placed on each desk and gives metrics for the required staff (or Full Time Equivalents) during the ramp-up and steady states.

POL00394097

- This model is used for forecasting and scheduling changes to the environment which could impact the Quality of Service provided at the Branches. It is owned and maintained by Operations.

No integration has been established between these models. In addition, neither gives an end-to-end view of the new environment.

3.6.3 Conclusions

a) At present capacity planning within POL is largely focussed on performing the business process –i.e. required headcount, desk-space and telephony equipment. The technical aspects of capacity are managed within each of the areas responsible for the delivery of those technical services, i.e. within the supplier organisations.
b) Although resources are allocated to a capacity management function within each platform area there is no overall picture of capacity requirements related to services delivered to the branches.
c) The suppliers within each platform area will be relied upon to deliver the necessary capacity inline with the levels contracted.
d) Monitoring of capacity utilisation after the implementation of development changes, to identify any differences between the forecast and actual requirements is not conducted across all platforms.
e) A capacity model has been prepared within POL to assess the impact of the Network Banking programme. This model focuses on the business aspects of the service, i.e. number of calls taken at the Service Desk. It does not provide information on the additional network and transaction loads generated by this increase in calls.

3.6.4 Recommendations

a) Consideration should be given to creating a process owner for the Capacity Management function. The resources currently allocated to this role for each platform should feed into this 'owner'. This would enable a picture of capacity utilisation, performance and requirements across all platforms to be established.
b) A single Capacity Plan should be compiled within the framework of the above Capacity Management process as it relates to and is appropriate for POL. This plan should encompass all platforms and all connectivity within the Network Banking environment through to the end users. This would ensure that the issues were considered and adopted from the beginning. It would also ensure that related service management processes are considered and interfaces built between them. The characteristics of the process should include:
    - Performance data, based on collected measurements and compared regularly with service levels
    - Ability to influence customer behaviour
    - Ability to predict capacity requirements with confidence
    - Involvement in application sizing
    - Influence with suppliers (and vendor management)
    - Assessment of project impact on resources
    - Data used as a basis for charging

POL00394097

- Data being fed into a Service Catalogue
- Data being fed into financial processes
- A feed into investment decisions
- Awareness of business plans
- More accurate budgeting
- Keeping track of savings and benefits that Capacity Management realises.

c) Consideration should be given to the development of an end to end capacity model for the Network Banking environment that focuses.

d) Steps should be taken to ensure that Network Support become involved in the lifecycle of projects to assess and advise on capacity requirements, to improve cost effectiveness, utilisation of resources and reduce the possibility of bottlenecks.

e) A virtual capacity team consisting of representatives from each area of the End-2-End environment should be established. A Bi-monthly meeting should be held and used as a forum for the discussion of capacity matters.

f) Consideration should be given to establishing a testing environment that enables the simulation of the live environment that covers all platforms for heterogeneous applications.

g) Notification of time-scales for stress testing within the supplier areas should be clearly defined; feedback from these tests should be fed to the central capacity management function within POL.

h) End to end capacity management workshops should be held with suppliers, focussing on: -
   - The tool sets used for performance and workload monitoring. If required, the plans should be made to enhance these tool sets.
   - Plans for stress testing in the pre-production environment, to determine the impact upon capacity resources.
   - The interfaces required between the supplier capacity processes and the central capacity management function within the Post Office.

i) Consideration should be given to utilising those tools currently used for reactive purposes, for real time performance monitoring.

j) Priority attention should be given to the current thoughts regarding the acquisition of additional tools, to monitor and trend performance of networks and associated equipment, particularly relating to modelling.

POL00394097

3.7 IT Service Continuity Management

3.7.1 ITIL Description

IT Service Continuity Management comprises the processes that deal with planning for extreme circumstances where the IT-service organisation is unable to supply the IT service provision in the normal way. The importance of Service Continuity lies particularly in ensuring the continuity of the IT service provision in the event of disasters. Service Continuity is responsible for preventing and rectifying the failure of an operation-critical IT service formally established within the organisation.

3.7.2 Introduction to IT Service Continuity Management

An ITSCM team is established within the Network Support business unit. The team is largely none technical. The focus of the process is primarily on ensuring that the supplier organisations and other internal business units deliver the contracted levels of continuity, inline with contracts. The main activities include: -

- Preparing of the continuity plan in accordance with the overall business continuity strategy.
- Performing quality assessments of each of the supplier continuity documents.
- Ensuring that supplier continuity tests are conducted inline with the provided test schedule.
- Ensuring feedback from these tests is reviewed and the necessary changes made to the continuity documentation.

A close working relationship has been created between Network Support ITSCM and Fujitsu Services. The interfaces between the two organisations are now mature and effective, having been steadily improved since the start of the contract. The required ITSCM interfaces have been formalised through the introduction of interface agreements defining the roles and responsibilities on each side.

To ensure that Main Business Continuity Incidents (MBCIs) are efficiently escalated to the ITSCM team a Trigger Guide document has been established. The NS Problem Management team, to ensure effective escalation of all MBCIs to the ITSCM team, uses this document.

3.7.2.1 Business Impact & Risk Analysis

Formal Risk Analysis techniques such as CCTA Risk Assessment Management Methodology (CRAMM) are not utilised by the NS ITSCM team. The analysis of the risk of disaster is largely dependent on the knowledge of the individuals within the ITSCM team.

POL00394097

3.7.2.2 Contingency plan

An overall contingency plan exists within POL. This plan is controlled through change control and is structured according to the POL Business Continuity Plan Standards.

The ITSCM team ensures that all supplier contingency arrangements are documented and copies stored within the NS CMDB.

3.7.2.3 Testing & Return to Base

The Fujitsu Services testing schedule is passed to the NS ITSCM team in November of each year. Members of the team are not required for each supplier continuity test; however the feedback is fed back to the NS ITSCM process where it is reviewed.

Supplier continuity plans are quality assessed and scored by the NS BCM team. Each document and its subsequent revisions are stored within the CMDB. Regular, scheduled tests are conducted against each of the supplier continuity plans to assess: -

- The conformance of the document to POL Continuity plan standards.
- If the plan is 'fit for purpose'.

Feedback from the tests is delivered to the supplier organisations. The team, following the same process, reassesses all subsequent revisions to the document.

3.7.2.4 Preventive action

Technical resilience is built into the architectures of each of the platform areas. In addition, the NS ITSCM team will assess and make recommendations on the continuity measures within the end to end environment.

3.7.3 Conclusions

a) The NS ITSCM process within the current environment is mature and effective. A transition plan is currently in place to extend the scope of this process to cover each additional supplier within the planned E2E environment. A four stage transition is planned:
   - **Stage 1** - Conduct Service Provider Continuity Assessments
   - **Stage 2** - Definition of the NS E2E Continuity Strategy
   - **Stage 3** - Establishment of Interface Agreements with each external Service Provider
   - **Stage 4** - Establishment of Interface Agreements with each internal Service Provider

b) The team has completed the product descriptions and is currently on target to ensure that the NS ITSCM process will meet the needs of the new environment.

POL00394097

c) The team members interviewed are well trained and knowledgeable on their subject. As with many small teams, specialists have developed within different continuity areas, this dependency on key individuals is seen as a risk.
d) The team has been invited to give feedback on the continuity measures within the agreed design of the Network Banking environment; however they are concerned that the project time-scales will not enable any initiatives recommended by the team to be acted upon.

3.7.4 Recommendations

a) Knowledge Transfer within the team is largely ad-hoc although workshops do take place. These knowledge workshops should be formalised occurring monthly.
b) To further improve knowledge retention within the team a knowledge base should be established. This will exist in addition to the NS CMDB, and may take the form of a shared network drive accessible by each team member. Background documents along with the output from each knowledge workshop should be placed on the ITSCM Knowledge Base. To aid access to this drive, a document index should be prepared and maintained by the team.
c) A virtual ITSCM team consisting of representatives from each area of the End-2-End environment should be established. A Bi-monthly meeting should be held and used as a forum for the discussion of continuity matters.
d) To further strengthen the process, more focus should be placed on understanding the technical continuity measures employed by each of the suppliers. This will require the development of additional technical skills within the team.
e) The minimum levels of operation to be delivered in the event of a disaster should be communicated to the business. This will ensure that expectations of both the business and the branches are managed.
f) Consideration should also be given to carrying out a simulated disaster to measure to assess the effectiveness of each supplier's continuity arrangements.
g) POL should ensure that they maintain the final approval of the invocation of supplier disaster recovery procedures.
h) A procedure should be implemented that creates a link between contingency planning and Change Management. The procedure should cover updating contingency plans, with recovery details of any new services or enhancements to existing services. All changes, particularly new projects, should be assessed with respect to their impact on the DR Plan.

POL00394097

3.8 Service Level Management

3.8.1 ITIL Description

The goal for Service Level Management (SLM) is to maintain and improve IT service quality, through a constant cycle of agreeing, monitoring and reporting upon IT service achievements and to instigate actions to eradicate poor service – in line with business and/or cost justification. Through these methods, a better relationship between IT and its Customers can be developed.

The future SLM process for Network Banking (NB) should ensure that:

- The NB service is designed to meet Service Level Requirements
- It enables improved relationships with satisfied customers.
- All parties to the agreement have a clear view of roles and responsibilities relating to the NB service and that there are no misunderstandings or omissions.
- There are specific targets to aim for and against which service quality can be measured, monitored and reported on (if you can't measure it you can't manage it and if you can't manage it you probably don't care!).
- IT effort is focused on the areas that the business believes are key.
- IT and customers have a clear and consistent expectation of the level of service required from NB. Priorities are agreed and understood.
- Weaknesses are identified through effective service monitoring by the suppliers, so that remedial action can quickly take place.
- Service monitoring by the suppliers should also show where Customers or User actions are causing the faults within NB and identify where working efficiency and /or training can be improved.
- It underpins the supplier management for the NB service
- The SLA should be used for a basis for charging for the NB service and therefore help demonstrate the value that the Customers are getting for their money.

3.8.2 History of Service Level Management within Post Office Ltd (POL)

SLM within POL was created within NS to support the Horizon contract. Since its inception, it has developed into a mature unit within Network Support and is responsible to ensure that SLA's and OLA's are consistently met in order that the service offered to its Customers by Fujitsu Services (ex: ICL Pathway) is of the best quality achievable.

3.8.3 Introduction to Service Level Management

Within NS there is a Supplier and Performance Management Team, responsible to ensure that the services provided are measured, monitored and managed to enable the delivery of business benefits to POL Customers. The team consists of a Service Level Manager and 8 staff.

There is no ITIL compliant Service Catalogue, but the information that would normally be used to populate such a catalogue is available, but not necessarily in

POL00394097

one place. The Service Catalogue would normally contain details of all services provided including:

- Business priority
- Service Name
- Version Number
- Service Description
- Service Hours
- Availability Target
- Back up details
- System Owner
- Key Contact

There are plans to further enhance the SLM team, albeit the plans were created for the existing services and not to cater for Network Banking

A new SLA is currently being developed that will cater for Commercial, Directly Managed and Social Offices.

3.8.3.1 Negotiate and agree SLA's

There is no specific Services Management Team, dealing with Customers. This is currently catered for within the SLM team.

User Review Group Forums are held in 10 locations every 6 months. At these events a mixture of staff come together and are invited to comment on the services provided by NS. NS conduct an additional forum every 1 to 2 months with Retail

Customer satisfaction surveys are conducted for the NBSC desk, but not for the Fujitsu Services Pathway service. Individual engineers do however leave a survey form when they visit outlets for maintenance purposes.

3.8.3.2 Managing Service Levels

NS make use of a Codified Agreement to define each element of the services provided by Fujitsu Services. This includes information regarding Service Level Agreements (SLA's). For example POCL Infrastructure (which is very comprehensive) contains the following:

- Service Definition
- Acceptance Criteria
- POCL Responsibilities
- Roll Out and Implementation
- Service Management
- Service Transfer
- Service Levels and Remedies
- POCL Contingency Services

POL00394097

There is a Service Review Framework in place (currently under review), for the Automated Network incorporating Horizon. This contains information regarding service review processes:

- between POCL and ICL Pathway
- between POCL and Post Office Customer Management Ltd. (POCML)
- review processes internal to POCL, which feed the service review hierarchy
- review processes which incorporate relevant interfaces with IT

Also contained within the Framework are sections on the following:

- Service Review Structure
- Service Management Forums (including Horizon Service Review Forum, Automated Services Forum, Operational Level Forums)
- New Requirements
- Operational Processes Forum (Problem Management, Business Continuity etc.)
- Systems Groups (Transaction Data Forum, Reference Data Forum etc.)
- Etc.

A number of Support Processes are included in the service review, namely

- Incident Management
- Problem Management
- Change Management
- Service Improvement Process
- Risk/Issue Management Process

The SLM team have created a matrix containing the key targets for service availability for each supplier. This is an excellent method for understanding the commitments required for the NB service.

3.8.3.3 Management Information

Suppliers have their own scorecard. There are over 100 different service targets for Fujitsu Services alone that contribute to their scorecard.

Suppliers provide information to POL on a monthly basis

Fujitsu Services Pathway now provide a trusted service and report by exception in their monthly service review

Some information is sent to the user community via publications. This usually consists of particular events that have happened relating to the services
Additionally some MI is sent out prior to the User Review Group Forums

POL00394097

3.8.4 Conclusions

a) There is a very competent and professional SLM function in existence within NS. However the existing structure may not be able to cope with the demands of the NB service. There will be a requirement to enhance the current SLM team for NB. This may be in numbers, but could also be in expertise.
b) There is no ITIL conformant Service Catalogue in existence. For the NB services such a catalogue would be invaluable to NS and the POL organisation in general.
c) The new SLA being developed for Commercial, Directly Managed and Social Offices will prove useful in managing suppliers and customer expectations.
d) There are no even handed (neutral) individuals between the business areas and SLM to report on service, or act as customer champion when issues arise.
e) With the implementation of NB, it will be necessary for SLM to conduct Customer satisfaction surveys, in order to gauge satisfaction with the service. Output from this can then be used as input to a Service Improvement Programme.
f) There are Service Level Agreements (SLA's) in evidence for the services currently managed by Fujitsu Services on behalf of POL. These form part of the Codified Agreement.
g) There is a comprehensive Service Review Framework in place that is used to good effect by the SLM team and contributing areas
h) The matrix created for the Network Banking key targets will be very useful and will enable the SLM team to see at a glance what the suppliers are committed to and therefore be able to manage them accordingly.
i) Management Information is provided and distributed by NS to the recipients of the current service.

3.8.5 Recommendations

a) SLM is a critical function and should continue to be totally owned and controlled by NS for the NB service. However the SLM function may employ the Fujitsu Services TSD to collect service data on its' behalf from the various suppliers.
b) A comprehensive project plan (PRINCE2) for managing the SLM functions for NB needs to be instigated and will include:
    - Appointing the new members of the team. The current staffing may need to be enhanced to support the NB service.
    - Define the roles, tasks and responsibilities.
    - Production of a Mission Statement for the new team to encourage focus and commitment.
    - Definition of the objectives and scope of the new function
    - Starting an awareness campaign to win support and advise people of their commitment and attain support.
    - Quantifying the activities, resources, funding and quality criteria
    - Consideration of implementing a Service Catalogue and agreement of the SLA structure

POL00394097

- Identifying any support tools for SLA monitoring. In the case of NB, these may be provided by the relevant suppliers
- Setting and agreeing Incident priority levels and escalation paths, with customers and Internal and External suppliers. This will have to be done in conjunction with the relevant suppliers Service Desks and Problem Management functions

c) The SLA currently being developed for Commercial, Directly Managed and Social Offices needs to include the requirements for NB.

d) Consideration should be given to appointing a NB Service Manager who will ensure End to End protection and assurance of the service on behalf of the customers.

e) Within 3 months of the launch of the NB service, a survey of the key customers should be undertaken and published within POL. This should form the basis of a Service Improvement Programme. The exercise should be repeated 6 months later.

f) The Codified agreement needs to be extended to include the NB service.

g) The Service Review Framework needs to be restructured to include the NB service. A whole new structure of Operational, Service and Contract review forums needs to be instigated with the following:
   - Fujitsu Services
   - I.B.M.
   - LINK
   - Alliance and Leicester
   - E.D.S.
   - Consignia Customer Management (C.C.M.)
   - Business Systems Business Unit (B.S.B.U.)
   - Post Office Ltd.

POL00394097

4 Costs

In the proposal dated March 4th 2002, there were some cost estimates given for undertaking a Service Development programme that would move the current organisation to a more mature level in terms of Service Management processes. These costs have now been refined in light of the recent work and as requested by POL, a cost matrix has been produced.

4.1 Cost Matrix

The following cost matrix summarises the investment that POL will have to make in order to support the Network Banking service. The matrix shows three states of readiness:

Achievable Solution the level of maturity that can be achieved before the launch of Network Banking (6 to 9 months).
Desired Solution this is the desired maturity level (9 to 12 months)
Ultimate Solution the ultimate maturity level which would take approximately 18 months to achieve.

In summary the costs are as follows:

Readiness	Total Cost
Achievable	£728,600
Desired	£903,050
Ultimate	£1,474,475

These costs are given in more detail in the following table.

POL00394097

Cost Matrix for Network Banking Service Management

		ACHIEVABLE				DESIRED				ULTIMATE			
	Current Maturity	Level	Resource	Man Days	Cost	Level	Resource	Man Days	Cost	Level	Resource	Man Days	Cost
Process:													
Incident	C	I	PR	60	£49,500	I	PR	60	£49,500	O	PR	120	£99,000
			PO	60	£18,000		PO	60	£18,000		PO	120	£36,000
Problem	C	I	PR	60	£49,500	I	PR	60	£49,500	O	PR	120	£99,000
			PO	60	£18,000		PO	60	£18,000		PO	120	£36,000
Change	AW	I	PR	60	£49,500	I	PR	60	£49,500	O	PR	120	£99,000
			PO	120	£36,000		PO	120	£36,000		PO	180	£54,000
Config.	IN	C	PR	60	£72,000	I	PR	120	£144,000	O	PR	180	£216,000
			PO	120	£36,000		PO	240	£72,000		PO	360	£108,000
Release	C	I	PR	60	£49,500	I	PR	60	£49,500	I	PR	60	£49,500
			PO	60	£18,000		PO	60	£18,000		PO	60	£18,000
SLM	C	I	PR	30	£24,750	I	PR	30	£24,750	O	PR	60	£72,000
			PO	60	£18,000		PO	60	£18,000		PO	120	£36,000
Availability	A	C	PR	60	£72,000	C	PR	60	£72,000	I	PR	100	£120,000
			PO	60	£18,000		PO	60	£18,000		PO	180	£54,000
Capacity	A	C	PR	60	£49,500	C	PR	60	£49,500	I	PR	100	£82,500
			PO	60	£18,000		PO	60	£18,000		PO	180	£54,000
BCM	AW+	C	PR	30	£24,750	C	PR	30	£24,750	I	PR	60	£49,500
			PO	60	£18,000		PO	60	£18,000		PO	120	£36,000
Tools				120	£144,00			180	£216,000			240	£288,000
											Totals overleaf…		

Maturity Key: A= Absence, IN= Initiation, AW= Awareness, C= Control, I= Integration, O= Optimisation

POL00394097

Cont…	ACHIEVABLE		DESIRED		ULTIMATE	
Project Costs:						
Managing Consultant	90	£121,500	120	£162,000	180	£243,000
Project Support	90	£58,500	120	£78,000	180	£117,000
Director	6	£9,000	12	£18,000	18	£27,000
	Total PR	£774,000	Total PR	£987,000	Total PR	£1,561,500
	Discounted	£530,600	Discounted	£669,050	Discounted	£1,042,475
	Total PO	£198,000	Total PO	£234,000	Total PO	£432,000
	Grand Total	**£728,600**	**Grand Total**	**£903,050**	**Grand Total**	**£1,474,475**

For further details of the PinkScan maturity levels, see APPENDIX A – ITIL Best Practice Model and APPENDIX B – Process Maturity Overview

POL00394097

POL00394097

5 APPENDIX A – ITIL Best Practice Model

Phase	Description	Characteristics
Absence 0 - 0.9	Nothing present	
Initiation 1 - 1.9	Tangible developments on field of interest	• Policy statements at tactical level • Words but no deeds • No allocated means
Awareness 2 - 2.9	Allocated means	• Aimed at tool, 'tool solves all problems' • Positions created, but not defined • Reactive • Standardisation for the benefit of direct control
Control 3 - 3.9	Formalised	• Visible results • Management reports • Tasks and authorities defined • Active instead of reactive • Tuning demand and supply • Documentation • Formal planning
Integration 4 - 4.9	Clearly defined elements	• Clear direction • Active relations with other processes • Effective management reports • Improvements in significant steps • Links to strategic policy
Optimisation 5 - 5.9	Elements work optimally	• Proactive • Quality section • Continually monitored improvement • Policy integrated with business policy • Integral responsibility/self control • Innovation

POL00394097

6 APPENDIX B – Process Maturity Overview