

# Systems Management Domain Roadmap

## Technology Roadmaps

### DOCUMENT CONTROL

#### Document Details

Document Owner	Tony Bright
Document Author	Neil Battell, Mark Cooper, Nick Morgalla
Current Version	1.1
Issue Date	23 <sup>rd</sup> April 2008
Programme Reference	Enterprise Architecture
Project Reference	Enterprise Architecture Systems Management Domain

#### Revision History

DATE	VERSION	CHANGE DETAILS
14 <sup>th</sup> April 2008	1.0	Initial Version
23 <sup>rd</sup> April 2008	1.1	Incorporate initial feedback

#### Distribution

DATE	VERSION	DISTRIBUTION
14 <sup>th</sup> April 2008	1.0	Tony Bright, Kaila Munaweera, Phil Burnham and Terry Pyle for initial review
23 <sup>rd</sup> April 2008	1.1	Architecture Program Board

## TABLE OF CONTENTS

---

1.0	Introduction.....	4
1.1	Objectives.....	4
2.0	Executive Summary .....	5
2.1	Developing the Systems Management capability .....	5
2.2	Potential for Outsourcing .....	6
3.0	Systems Management Domain Architecture Description .....	7
3.1	British Council's Enterprise Architecture Approach .....	8
3.2	Position of the Systems Management Domain within the overall British Council Enterprise Architecture.....	9
3.3	Capability Summary .....	10
3.3.1	Monitoring and alerting mechanisms .....	10
3.3.2	Dashboard Management Information Systems .....	10
3.3.3	Enterprise Discovery Tools.....	10
3.3.4	Software distribution tools.....	10
3.3.5	Backup and restore mechanisms .....	11
3.3.6	Support tools including those facilitating remote support .....	11
3.3.7	Service Management tools aimed at facilitating and where possible automating IT processes .....	11
4.0	Direction of Travel .....	12
4.1	Business changes impacting the Systems Management Domain.....	12
4.2	Evolution into Service Management.....	12
4.3	IT changes impacting the Systems Management Domain .....	14
4.3.1	Increased centralisation of services and servers.....	15
4.3.2	Increased IP-based telecommunications traffic routed by the network provider .....	15
4.4	Technology opportunities .....	16
4.5	Overview of Change .....	16
4.5.1	Complete Current Rollout and Use Existing Tools .....	18
4.5.2	Service Management drivers .....	18
4.5.3	System Management priorities .....	19
5.0	Detailed Description .....	20
5.1	Logical Domain Model .....	20
5.2	Toolsets currently used .....	21
5.3	Physical Domain Model .....	24
6.0	Making it Happen .....	25
6.1	Technology Choices.....	25
6.2	Key Organisation Processes .....	25
6.3	Resources and Skills .....	29
6.4	Provision Assumptions .....	29
6.5	Milestones and Deadlines .....	29
6.6	Domain Strategic Roadmap .....	30
6.6.1	Step 1 – Complete SMS rollout .....	30

6.6.2	Step 2 – Implement integrated tools to support key ITIL processes	30
6.6.3	Step 3 – Implement Centralised Backup and Restore	31
6.6.4	Step 4 – Implement Performance and Experience Monitoring	31
6.7	Domain Technical Roadmap	31
7.0	Appendix 1 – Principles Guiding the Systems Management Domain	32
7.1	Business Principles	32
7.2	Functional Principles	32
7.3	Technical Principles	32
7.4	Implementation Principles	32
7.5	Governance Principles	32
8.0	Appendix 2 – Systems Management Domain Standards	32

## TABLE OF FIGURES

---

Figure 1 - British Council Enterprise Architecture Approach	8
Figure 2 - British Council Enterprise Architecture domains	9
Figure 3 - System and Service Management Interfaces	14
Figure 4 - Service Management processes and their links to System Management functional capabilities	17
Figure 5 - Service Management processes and their links to System Management functional capabilities	20
Figure 6 - Service Management processes	23
Figure 7 - Physical Domain Model	24
Figure 8 - People, Process and Product	26
Figure 9 - Systems Management Process Framework	27
Figure 10- Platform Domain High-Level Strategic Roadmap	30
Figure 11 - Domain Technical Roadmap	31

## TABLE OF TABLES

---

Table 1 – Systems Management Domain Strategic Approaches	5
--	---

## **1.0 Introduction**

This document describes the target architecture roadmap for the Systems Management Domain.

### **1.1 Objectives**

The objectives of this document are:

- To provide a summary of the roadmap for the Systems Management Domain
- To communicate an understanding of the Systems Management Domain target architecture to stakeholders at an appropriate level of detail
- To position the Systems Management Domain within the overall British Council enterprise architecture and describe the capabilities covered by this domain
- To describe how the business direction and technology opportunities have shaped the target domain architecture
- To explore the options available to British Council for this domain
- To identify the major deadlines and milestones for the delivery of the capabilities provided by this domain
- To identify at a high level the resources and skills required to implement the capabilities
- To describe the Systems Management Domain roadmap

## 2.0 Executive Summary

The British Council's enterprise architecture is currently organised into seven domains; data, applications, collaboration, platform, networks, system management and security. This document focuses on the systems management domain.

Because the UK infrastructure and global networks are outsourced, the systems management architectures for those elements are the responsibility of the service suppliers and out of scope of this document. However, consideration must be given to the system management interfaces between the service providers and the British Council.

Currently within the British Council, thirty different system management tools are used by nine different support entities. There is a real opportunity to simplify the systems management landscape, bringing potential cost savings and service improvements.

While some work has taken place within this domain, specifically the rollout of System Management Server (SMS), there is much more that can be done both in the short and medium term.

### 2.1 Developing the Systems Management capability

Priority	Initiative	When	Key Benefits
High	Complete SMS rollout	ASAP	<ul style="list-style-type: none"> <li>• Reduced support cost</li> <li>• Improved service quality</li> <li>• Reduced operational risk</li> </ul>
High	Implement standardised, integrated tools to support key ITIL processes: <ul style="list-style-type: none"> <li>• Incident management</li> <li>• Problem management</li> <li>• Service management</li> <li>• Security management</li> </ul>	By end 2010 <sup>1</sup>	<ul style="list-style-type: none"> <li>• Reduced support cost</li> <li>• Improved service quality</li> <li>• Reduced operational risk</li> <li>• Increased value from service providers</li> </ul>
Medium	Implement centralised backup and restore	By mid 2010	<ul style="list-style-type: none"> <li>• Reduced support costs</li> <li>• Reduced operational risk</li> </ul>
Medium	Implement performance and experience monitoring	By end 2011	<ul style="list-style-type: none"> <li>• Improved service quality</li> </ul>

**Table 1 – Systems Management Domain Strategic Approaches**

Completing the current rollout of SMS for the overseas platform is important and should be given high priority, especially since it is a dependency for the installation of critical software patches. Once implemented and integrated into the service management processes, it will provide a much-improved understanding of and strong control mechanism for the overseas platform.

<sup>1</sup> This timeline will be driven by the Service Management function; however, this is not unrealistic in term of implementing the tools.

Focussing on the four key ITIL service management processes (Incident, Problem, Service and Security Management) is most likely to provide initial benefits. Providing an *integrated* system to support these processes is a high priority. While currently some limited tool support exists for some processes, considerable benefit could be realised by taking an integrated approach, enabling information to be shared highly effectively.

*Service management* is outside the scope of enterprise architecture as defined for this project. It is important to align the service and system management architectures and roadmaps and not to develop either solution set in isolation.

Implementing centralised backup and restore will provide benefits in terms of reduced operational risk and reduced costs through automating the backup process. This will reduce the need for skilled on-site IT staff.

Finally, implementing performance and experience monitoring tools will provide benefits in terms of improved service levels to end-users and customers. However, there is a linkage with the ITIL processes and service management and system management roadmaps need to be aligned.

## 2.2 Potential for Outsourcing

The systems management roadmap has to be considered within the context of the potential for outsourcing the overseas platform.

If a decision is made to outsource the overseas platform, then much of the responsibility for the systems management architecture will pass to the service supplier. The timeline is therefore significant. The Council needs to decide whether each activity needs to be completed before any decision is taken on the precise outsourcing strategy in 2012. It would be highly complex to try to hand over projects “in flight” – the British Council would want to pass over to contractors a system that enables them to return the same or better efficiencies. It is recommended that the Council also explore NOW with potential service providers (including Flex) exactly what their service offers and whether there is any nugatory effort or cost in their current strategy.

On balance, and subject to those discussions, our view is that the projects should be completed and then the decision on outsourcing strategy taken since:

- it cannot be assumed that a more complete outsource will take place in 2012
- It cannot be assumed which provider will win the contract
- There are significant benefits even in the medium term of completing the designated projects

The above approaches are described in more detail in the following sections of this document.

### 3.0 Systems Management Domain Architecture Description

The Systems Management domain covers the tools required by the British Council to manage and support its IT processes and infrastructure, in a manner that is both effective and efficient. In terms of process, the British Council is actively working to adopt the Service Management best practices documented within the IT Infrastructure Library (ITIL), so this domain includes those tools required to support the ITIL processes.

While a strict definition of Systems Management would not necessarily include Service Management tools, there is significant overlap. Given the stage that the British Council has now reached in terms of Service Management, with a number of Process Owners looking for new tools, it makes sense to now bring these requirements together. This will facilitate the provision of an integrated tools architecture that supports the combined requirements in as efficient and cost effective manner as possible.

Currently the UK platform and global networks are outsourced, leaving the overseas infrastructure managed by British Council staff. This document assumes that the model does not change. If the model does change, the systems management requirements are likely to change too with much of the responsibility for the system management architecture passing to the service supplier.

In the current situation where for the UK platform and global network the service suppliers have responsibility for day-to-day operation and therefore system management tools, there is still a need for the British Council to have sufficient visibility and control across the overall infrastructure, in order to:

- Gain regular assurance that outsourced service components are being managed in accordance with contracted service levels
- Understand the end-to-end architecture of IT services in order to assess the impact of changes and support the design of future service improvements
- Gain assurance that both security and business continuity related risks are being appropriately managed
- Facilitate the proactive identification of faults and underlying problems within the infrastructure
- Allow IT Management to monitor the quality of service being provided to the business and end users
- Enable factors impacting security, performance, resilience and recoverability to be understood and taken account of during the design of future IT services

The major components that form the domain are:

- Monitoring and alerting mechanisms
- Dashboard Management Information Systems
- Enterprise discovery tools
- Software distribution tools
- Backup and restore mechanisms
- Support tools including those facilitating remote support

Over time, as the domain links into the Council's evolving Service Management framework:

- Service Management tools aimed at facilitating and where possible automating IT processes

### 3.1 British Council's Enterprise Architecture Approach

The Enterprise Architecture is a comprehensive framework used to manage and align an organization's business processes, Information Technology (IT), software, hardware and information requirements with the organisation's overall business strategy.

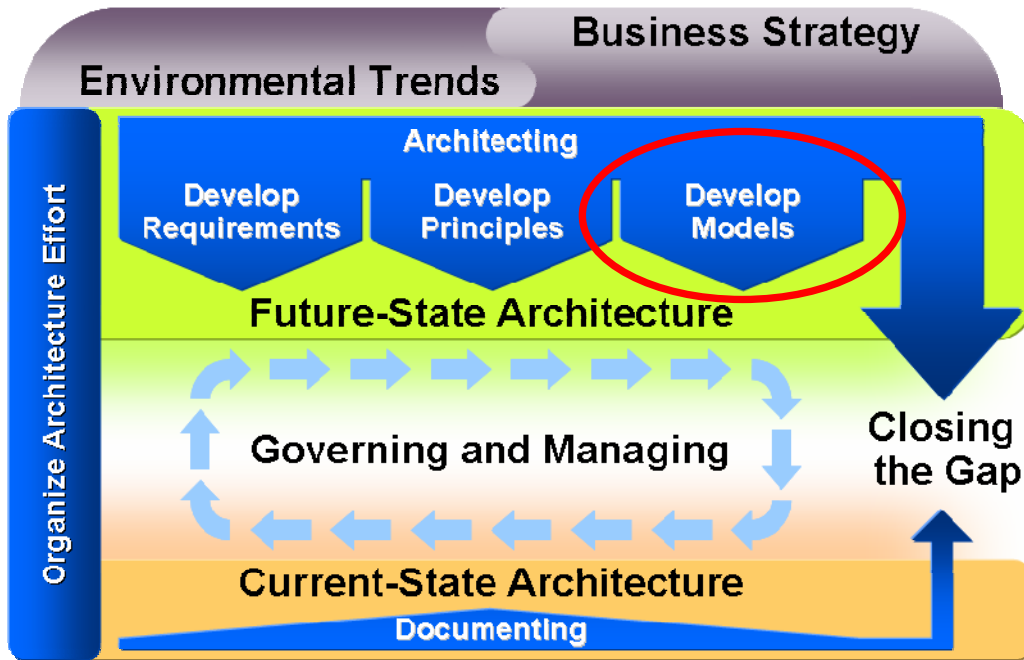


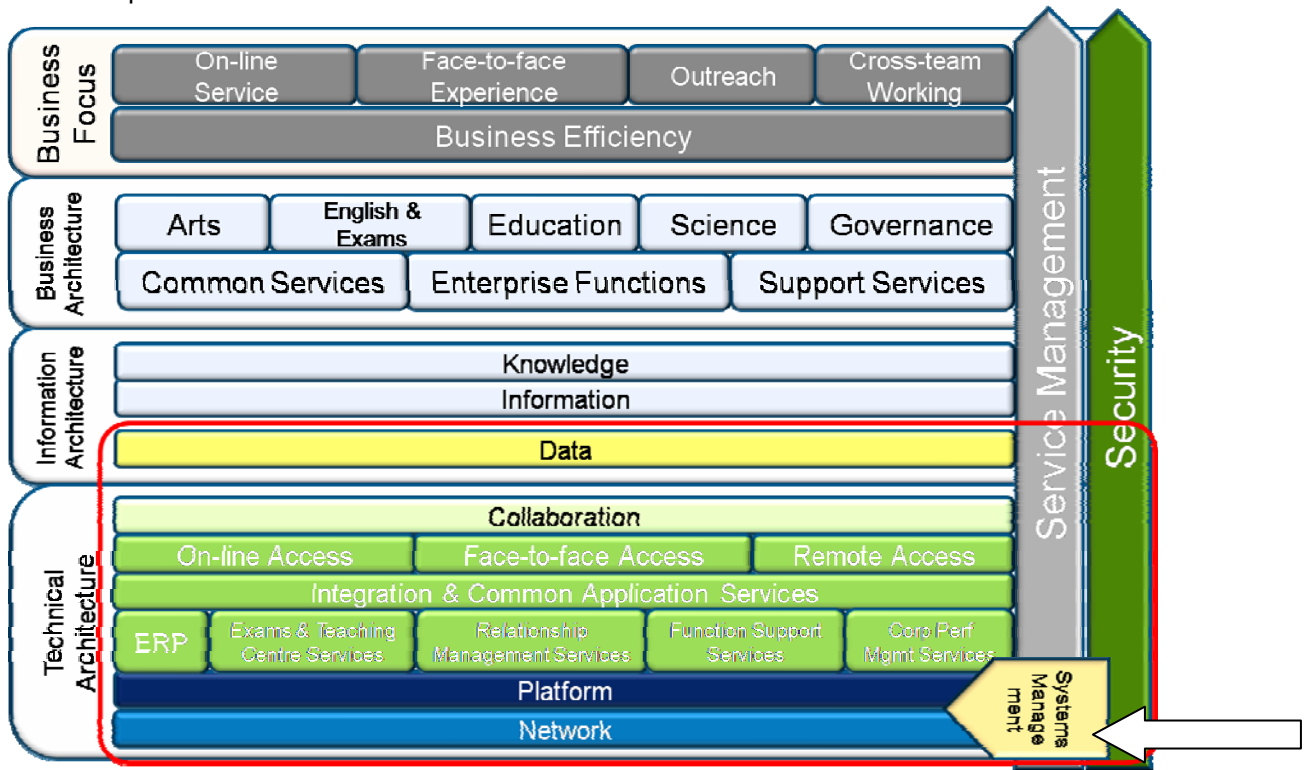
Figure 1 - British Council Enterprise Architecture Approach

This document focuses on developing the architecture model for the Systems Management Domain.

### 3.2 Position of the Systems Management Domain within the overall British Council Enterprise Architecture

The Systems Management Domain provides monitoring, support and management capabilities that can be utilised to manage components in all of the other domains. In this way, the domain is similar to the Security Domain, which also cuts across all other domains.

There is a close relationship between the Systems Management and the Security domains, as both are concerned with governing and managing IT systems, data and components across the British Council infrastructure. Both of these domains are dependent on the implementation and operation of appropriate processes in order to ensure that their objectives are achieved. The processes within these two domains should be integrated with each other to enable efficient and effective operation.



**Figure 2 - British Council Enterprise Architecture domains**

The systems management domain is one of seven enterprise architecture domains currently identified within the British Council. The 'in-scope' domains are shown within the red box in the picture above.

The Systems Management domain covers the tools required by the British Council to manage and support its IT processes and infrastructure. These capabilities are listed in detail below.

### **3.3 Capability Summary**

This section describes the key capabilities that will be delivered by this domain when the target state has been achieved. They are in no particular order.

#### **3.3.1 Monitoring and alerting mechanisms**

The capabilities under this heading will be utilised by the following processes:

- Incident Management
- Problem Management
- Capacity Management
- Availability Management

Key capabilities include:

- Event detection
- Filtering and aggregation of events
- Alerting on significant events occurring within the infrastructure
- Alerts based on appropriate thresholds against key utilisation metrics
- Scripted responses to significant alerts including the raising of Incidents
- Monitoring and recording of capacity related metrics
- Monitoring and recording of availability and performance related metrics

#### **3.3.2 Dashboard Management Information Systems**

The capabilities under this heading will be utilised by the following processes:

- Governance
- Service Reporting
- Continual Service Improvement

Key capabilities include:

- Taking of metrics data feeds from a variety of sources
- Aggregation of metrics and calculation of Key Performance Indicators
- Top level dashboard view for management information
- Drill down to allow investigation of underlying metrics

#### **3.3.3 Enterprise Discovery Tools**

The capabilities under this heading will be utilised by the following processes:

- Configuration Management

Key capabilities include:

- Detection of IT components
- Identification of key component attributes
- Integration to allow comparison of 'as is' configuration against the 'authorised' CMDB

#### **3.3.4 Software distribution tools**

The capabilities under this heading will be utilised by the following processes:

- Release Management
- Patch Management

Key capabilities include:

- Remote server, desktop and laptop builds to facilitate swap-out
- Remote distribution and deployment of standard software applications
- Remote distribution and deployment of optional software applications on demand
- Automated deployment of approved patches including security patches

### **3.3.5 Backup and restore mechanisms**

The capabilities under this heading will be utilised by the following processes:

- Availability Management
- Service Continuity Management
- Incident Management

Key capabilities include:

- Automated backups
- Remote backup
- Remote restores
- Alerting on backup failure
- Cataloguing of backed up files
- Handling of open files
- Compatibility with DBMS versions in use

### **3.3.6 Support tools including those facilitating remote support**

The capabilities under this heading will be utilised by the following processes:

- Incident Management
- Problem Management
- Capacity Management

Key capabilities include:

- Remote control of servers, desktops and laptops
- Detailed performance analysis

### **3.3.7 Service Management tools aimed at facilitating and where possible automating IT processes**

The capabilities under this heading will be utilised by the following processes:

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management

Key capabilities include:

- Logging and tracking of Incident records
- Logging and tracking of Problem records
- Recording and maintenance of Configuration information
- Logging, tracking, assessment, authorisation and scheduling of Change records
- Use of configuration information to assess change impact

- Tracking and scheduling of Release records
- Linking of records including:
  - Problems to associated incidents
  - Changes to related incident or problem records
  - Parent to child changes
  - Releases to associated changes

## 4.0 Direction of Travel

### 4.1 Business changes impacting the Systems Management Domain

The strategy of changing the operating model for overseas sites and pulling back the servers where possible to the UK has a significant impact on the Systems Management Domain, as this transfers much of the responsibility for these servers to the outsourcing company.

Any future change to the site operating models or the sourcing strategy (outsourcing or in-sourcing services) will potentially affect the Systems Management Domain. In terms of the current sourcing strategy, the Systems Management requirements can be broken down into two main groupings:

- Those for in-house managed components, applications and services
  - LANs, servers and desktops within overseas offices
  - Web (online) services
  - Other British Council supported applications, services and components
- Those for outsourced components and services
  - UK infrastructure (the desktop environment and LAN) (Logica)
  - Global WAN (Global Crossing)
  - SAP (HP)
  - Multiple web hosting providers

The British Council needs to have sufficient Systems Management capabilities in order to directly monitor, manage and support the IT service components that are not outsourced. For the outsourced service components, the British Council needs to have:

- Assurance and configuration knowledge from the service provider, in the form of:
  - Real time monitoring and alerting. This may be via view access into the service providers' tools or via a data feed from their tools
  - Regular reports including ones covering service exceptions
- Independent confirmation of service levels against contractual requirements
  - Reported service levels should be verified using the British Council's own tools or other such independent means

### 4.2 Evolution into Service Management

The Systems Management Domain and the wider Service Management strategy should act as key enablers for the increased focus on efficiency and reduced IT costs:

- Systems Management tools will increase efficiency through the automation of many manual tasks, such as logging on to systems to check that services are running or that backups have been successful
- Service Management best practices have been used by many organisations to reduce costs and increase efficiency. Examples include:
  - Tighter control and management of Configuration Items (CIs) such as desktops and laptops, leading to more optimal use of existing resources and reduced theft or loss of devices
  - Increased control of software and licenses, again allowing more optimal use of existing resources but also reducing costs by not paying for software that is no longer used
  - Increased understanding of how services are used and the costs of delivering specific services. This has allowed organisations to build more cost effective services while retiring services that are no longer viable
  - Reduced cost of downtime through designing for availability, the proactive identification and rectification of problems, appropriately prioritised response to incidents and improved assessment of change requests
  - Improved use of staff time through a reduction in repeat incidents, reduced incidents as a result of changes, and less confusion caused by a lack of consistent process and procedures
- Service Management tools increase efficiency by helping automate and govern the operation of the IT processes. An integrated Service Management toolset, supports the efficient integration of the processes and significantly reduces the cost and effort of doing bespoke integration between a number of disparate tools

There are currently a number of tools used to record the Incidents, Service Requests and Change Requests occurring within the British Council infrastructure.

As the British Council's Service Management capability develops, increasing importance and value will be placed on the Service Management tools, such as Remedy and ServiceCenter. As such, a toolset is used; a detailed IT knowledge base builds up containing:

- Incidents that have occurred and how they were resolved
- Workarounds that have been used successfully for past Incidents
- Problems that have been identified, how they were diagnosed and then resolved
- Known Problems and Errors within the infrastructure
- Changes that have been implemented, including why they were required, how they were assessed, who approved them and how they were implemented
- Releases and their contents
- The status of CIs, their relationships and the audit history of changes made to each CI
- The service levels that have been achieved
- Historical data allowing trends in Incidents, Service Requests and Changes to be examined and used for planning purposes

It is important to realise the value of this knowledge base to the British Council. This highlights two main issues:

- Ongoing ownership of the tool and its data. The information is valuable and should be 'owned' by the British Council

- The value of having all of this information in one place allowing one consistent view of the whole IT 'picture', rather than scattered across a number of different tools so that only part of the 'picture' can ever be seen.

The recommended strategy should be to move towards a single integrated Service Management toolset, owned by the British Council and accessed by all relevant outsourced service providers. The model for access by service providers should be standardised and contractually agreed, including where feasible any automated integration with the service providers own management systems. This should provide the right level of information and business decisions to the required functions, irrespective of whether they are delivered internally or externally. It also helps ensure that the Council can control the situation in the event of contractor failure or termination.

The diagram below shows the projected relationship between the System Management and Service Management layers, both within the British Council and between the British Council and its third party service providers.

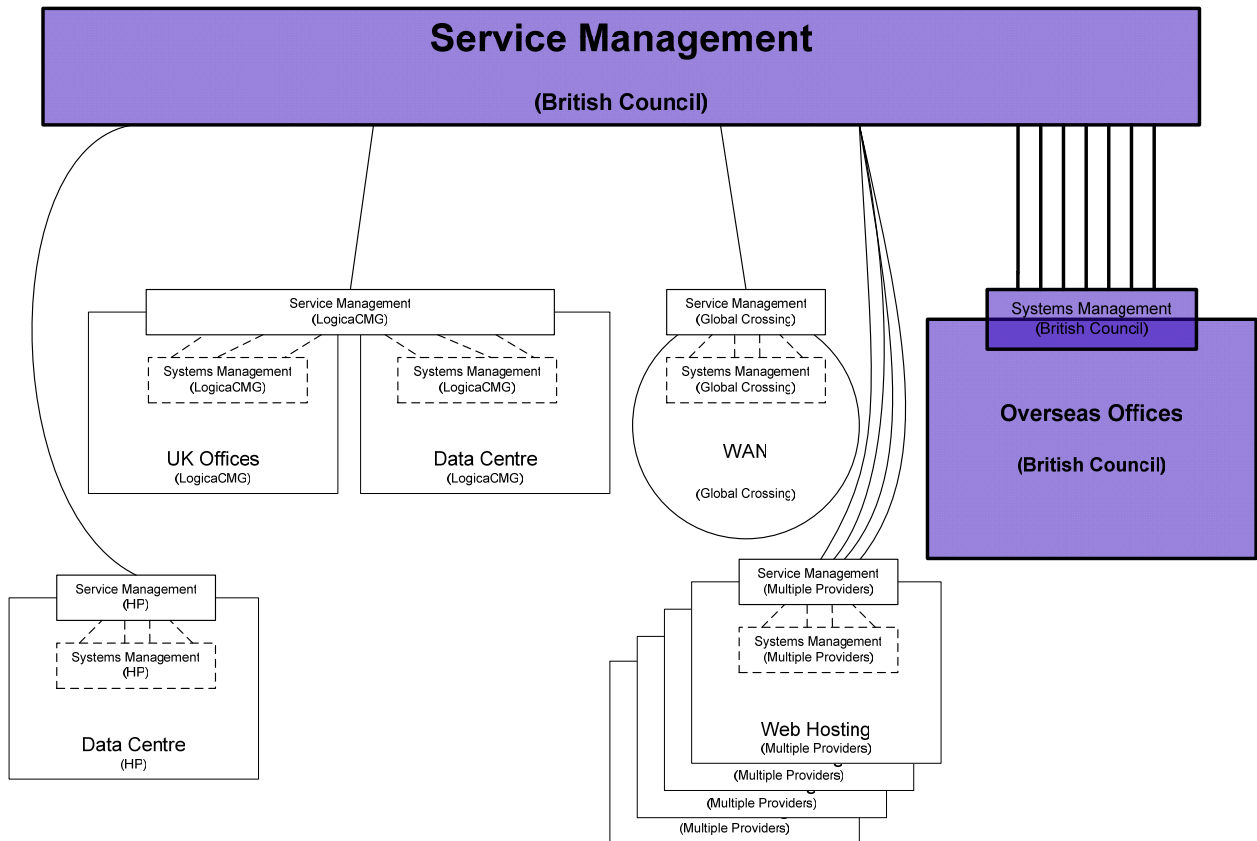


Figure 3 - System and Service Management Interfaces

### 4.3 IT changes impacting the Systems Management Domain

There are two main architectural IT changes that are likely to occur that will have an impact on the systems management domain. These are:

1. Increased centralisation of servers and services (consolidation/virtualised desktop infrastructure (VDI)/thin clients...)
2. More telecommunication traffic being routed by the network provider (Global Crossing)

The impact of these expected changes is described below.

#### **4.3.1 Increased centralisation of services and servers**

There is a move to reduce the number of server's deployed world wide and, where possible, to host the remaining servers and services in a central data centre in the UK. Work is already underway, with the centralisation of Microsoft Exchange services into the LogicaCMG facility being one example. Please refer to the Platform Domain Roadmap document for more details of the proposed centralisation of servers.

Such centralisation will affect the environment in a number of ways:

- There will be a higher dependency on the outsourced platform hosting company to monitor and maintain what will come to represent the bulk of the British Council's IT infrastructure. Any failures by the hosting company could now affect a far greater proportion of the British Council's business services.
- There will be a higher dependency on the global network provider to maintain global network services into and out of the hosting company's data centre. Again, any failures by the network provider could now affect a far greater proportion of the British Council's business services.

There is a linkage between the management of service that takes place within each service provider and the overall service management that takes place with the British Council. This has implications on the systems management architecture, in particular ensuring that information is provided and integrated between the various service suppliers at the appropriate points and times.

#### **4.3.2 Increased IP-based telecommunications traffic routed by the network provider**

There is a drive to rationalise the voice telephony infrastructure and suppliers, probably standardising on using Global Crossing as the sole supplier. There is a concurrent investigation to simplify the diverse and distributed infrastructure through the introduction of a few large centralised intelligent voice switches.

Each of these changes would place a higher dependency on the network provider (currently Global Crossing). Again, any failures by the network provider would now affect a far greater proportion of the British Council's business services, affecting not only data but now also voice communications.

In both of the potential situations outlined above, Systems Management, and in particular the Supplier Management process, will play a crucial role in ensuring the operational stability of the British Council's critical business services.

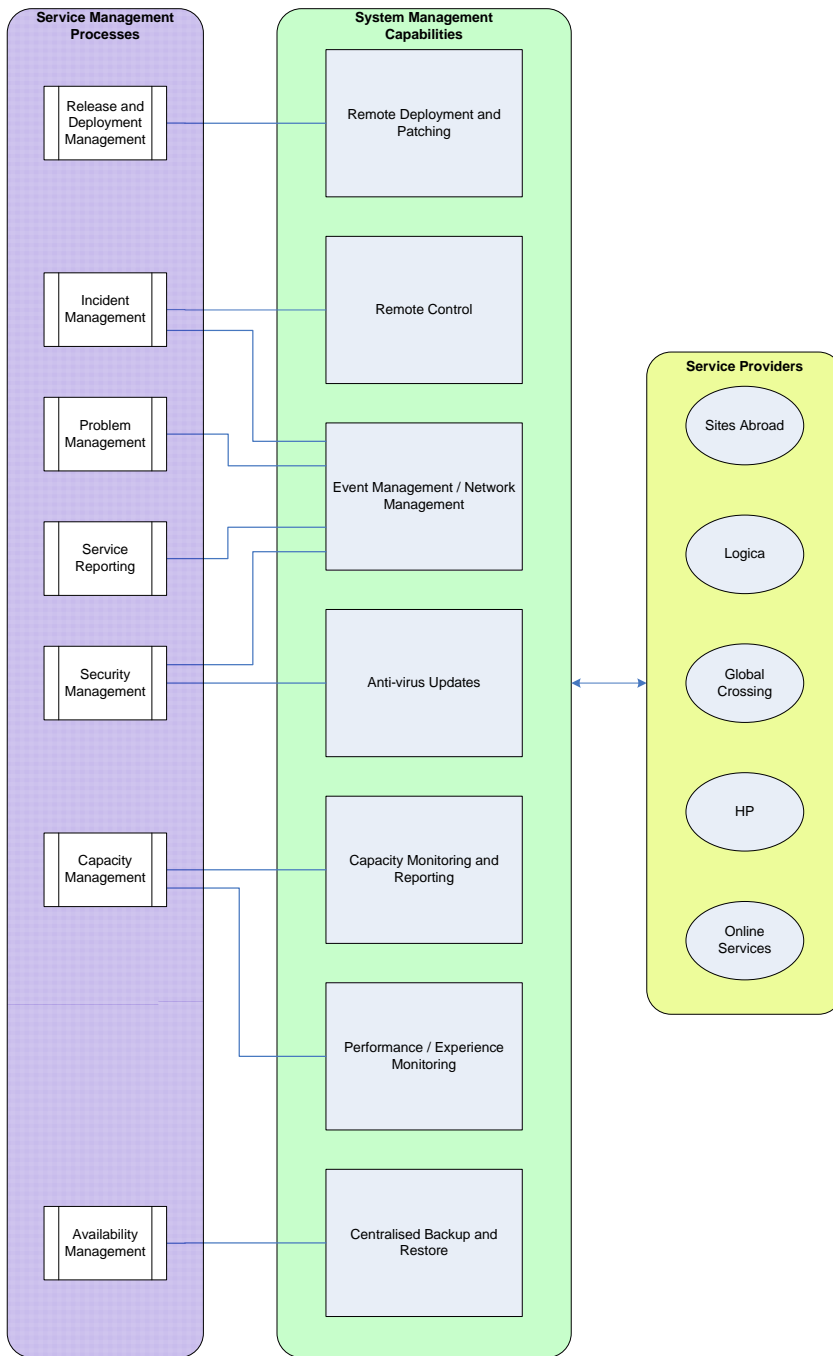
#### **4.4 Technology opportunities**

The existing and emerging technologies that will influence and enable the domain to deliver greater business benefit include:

- Microsoft Systems Centre
- Developments in CMDB and enterprise discovery tools, allowing change verification and the improved identification of unauthorised changes
- ServiceManager v7 now exists as a replacement for ServiceCenter
- SAP
- Federated CMDB models using tools such as future versions of uCMDB
- Application discovery / mapping technology and improving dashboard solutions to provide management information based on business service views

#### **4.5 Overview of Change**

The diagram below shows the linkages between the key Service Management processes and Systems Management functional capabilities



**Figure 4 - Service Management processes and their links to System Management functional capabilities**

In the diagram, the Systems Management capabilities (central boxes) can be categorised as:

- A) Exist and used
- B) Exist but not used
- C) Don't exist

The capabilities that exist and are used are:

- Remote Deployment and Patching
- Remote Control
- Antivirus Updates

The capabilities that have not been uniformly implemented are:

- Event and Network Management
- Capacity Monitoring and Reporting
- Performance and Experience Monitoring
- Centralised Backup and Restore

#### **4.5.1 Complete Current Rollout and Use Existing Tools**

There are a number of initiatives currently underway that are beneficial to the Systems Management domain. For instance, the rollout of Microsoft SMS, which is nearing completion, will enable a number of key features including the ability to automatically deploy software and patches and to discover and manage system configurations.<sup>2</sup>

Additionally, a number of facilities are available that are not currently being utilised. For instance, many of the overseas servers have built-in "lights out" capability. Subject to suitable cabling being configured, these servers can be powered on and off remotely, eliminating the need to have local staff available simply to push power switches.

Drawing up a list of similar under/non-utilised facilities might highlight additional opportunities to increase efficiency and reduce operating costs.

#### **4.5.2 Service Management drivers**

While there are a few instances where the implementation of Systems Management processes are already supported by technologies, many more are still lacking such support. Clearly, there is a need to invest in additional Systems Management tools. However, the prioritisation of such investment is best driven by the Service Management roadmap.

The key Service Management processes<sup>3</sup> are Incident Management, Problem Management, Configuration Management, Change Management and Release Management. Based on previous experience, the most common priority is:

1. Incident Management
2. Problem Management

---

<sup>2</sup> A number of key BAU activities are on hold pending the completion of the SMS roll out, one in particular being cause for concern. This is the delayed roll out of Microsoft's recommended critical patches. These patches typically address serious security and stability issues in the Microsoft operating systems. The delay, believed to be in the order of 12 months at time of writing, leaves the Council vulnerable to a wide range of exploitable threats.

<sup>3</sup> ITIL v2

3. Availability Management
4. Capacity Management

After Incident and Problem Management, the order of implementing the processes and supporting technologies is usually driven by analysis of the results of Problem Management. However, given that some of the Systems Management tools required to support Availability Management and Capacity Management are already in place, implementing the remaining requisite tools would represent the most efficient investment.

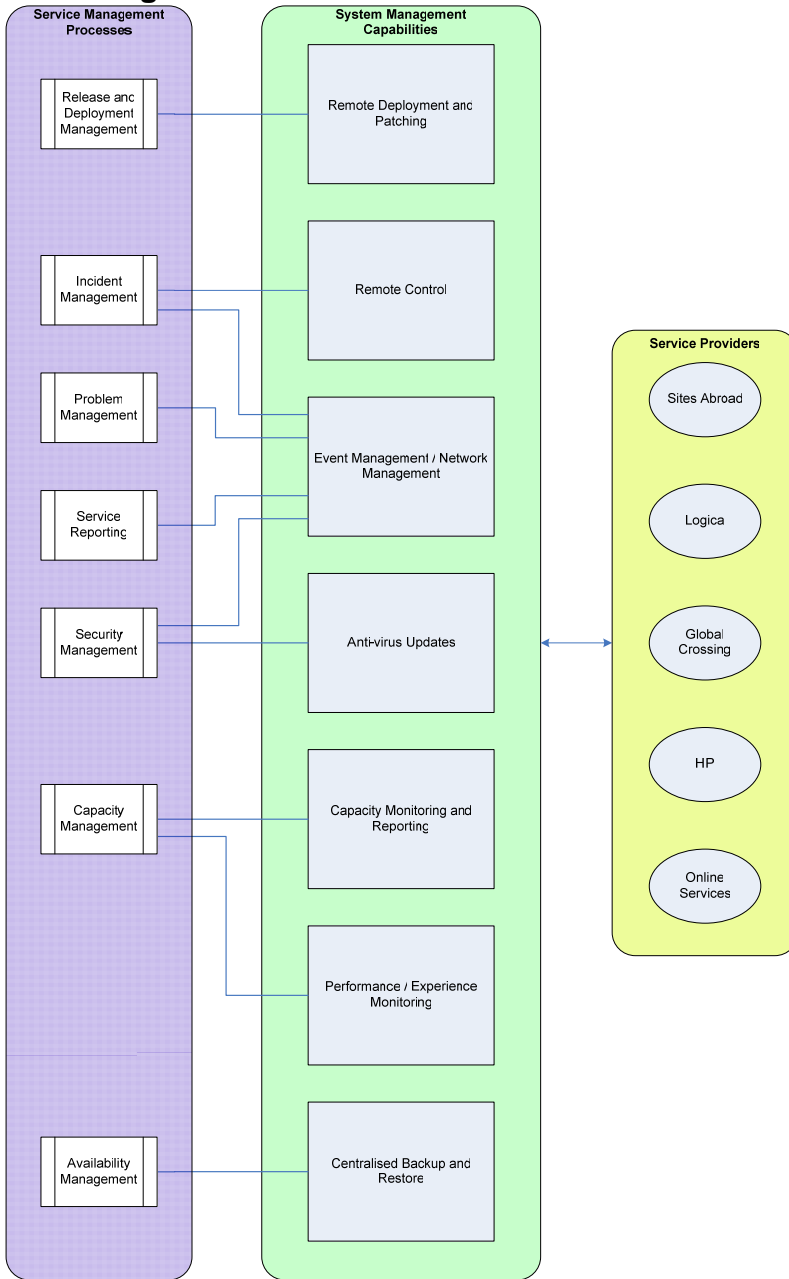
#### **4.5.3 System Management priorities**

Examining Figure 4 together with the expected Service Management priorities from section 4.5.2 above leads to the following prioritisation for developing additional Systems Management capabilities:

- 1) Event and Network Management capabilities are required by four separate Service Management processes. It therefore suggests that prioritising on these capabilities would provide an efficient return on investment, enabling Incident Management, Problem Management, Service Reporting and Security Management.
- 2) Implementing a Centralised Backup and Restore capability would assist availability management. It is understood that investigations are already underway.
- 3) Performance / Experience Monitoring and Capacity Monitoring and Reporting are required to successfully implement Capacity Monitoring as a Service Management process. The order in which these two capabilities are tackled is likely to be determined by analysis of the knowledge generated by the Problem Management process.

## 5.0 Detailed Description

### 5.1 Logical Domain Model



**Figure 5 - Service Management processes and their links to System Management functional capabilities**

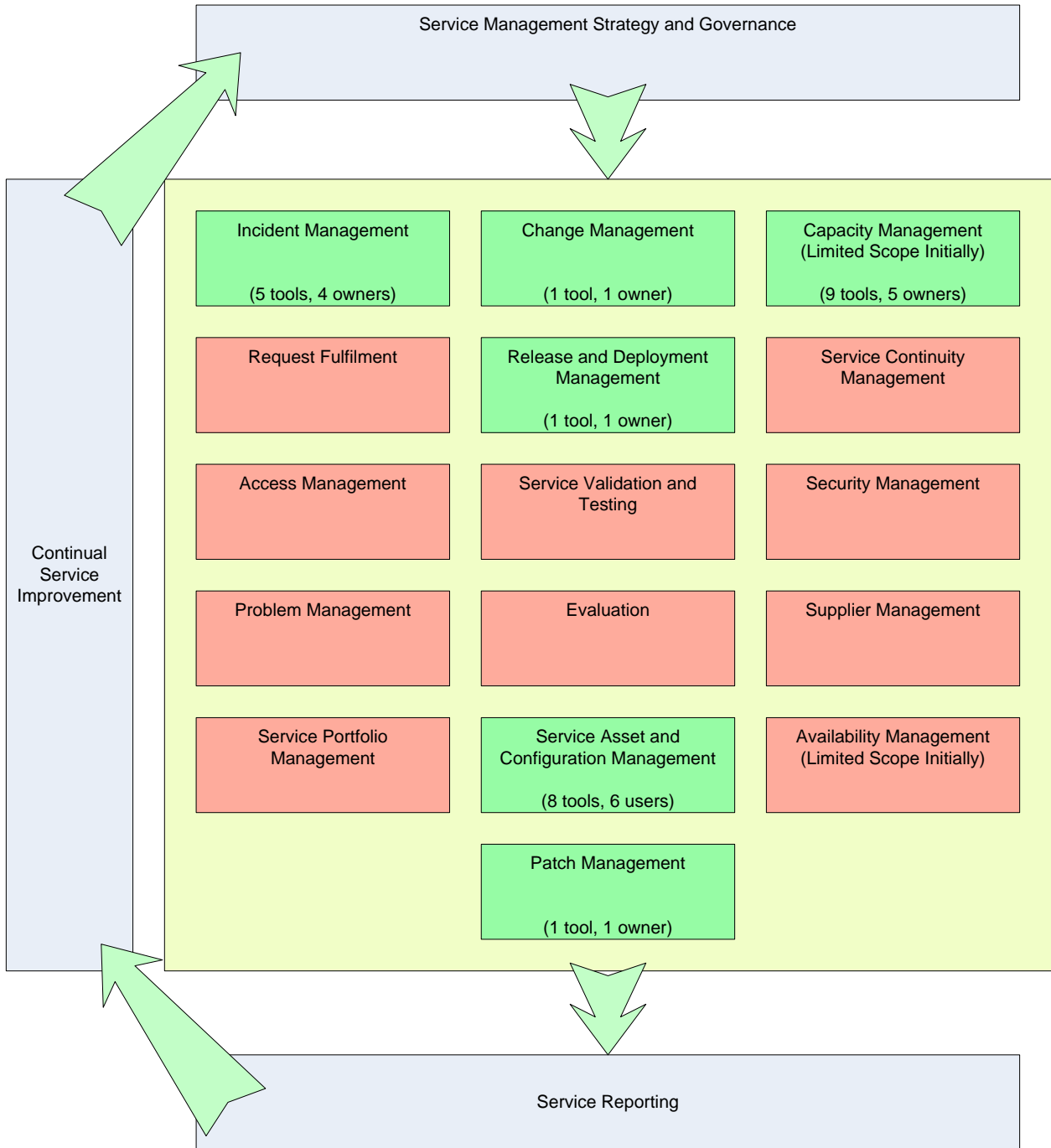
### 5.2 Toolsets currently used

There are currently different 30 tools used by nine different support entities. This is summarised in the table below.

Category	Application	Used By
Assets Management - Hardware	Dell Open Manage	Oversees
Assets Management - Hardware and Software	SIT Database	BAU / Oversees
Assets Management - Hardware and Software	Microsoft Systems Management Server	Globally
Assets Management - Software	ADU Time Database	BAU
Assets Management - Software	ELT Software Review database	E&E / Oversees
Assets Management - Software Licences	Centennial Discovery	LCMG
Assets Management - Licence	Phonex DashBaord	LCMG / GIS
Assets Management - Licence	Phoenix Audit Cleanse	LCMG / GIS
Change Management / Release Management	miManager	GIS
Configuration Management	Visual SourceSafe 2005	BAU
Configuration Management	Visual Studio Team edition	BAU / ADU
Configuration Management - Hardware	HP iLO	LCMG
Configuration Management - Software	Microsoft Systems Management Server	Globally
Configuration Management - Software	Updater	Globally
Incident Management - Service Desk	FogBugz	BAU
Incident Management - Service Desk	Service Centre	E&E
Incident Management - Service Desk	WebTrust	E&E
Incident Management - Service Desk	SAP Solution Manager	FABS
Incident Management - Service Desk	Remedy	LCMG
Patch Management	Microsoft Systems Management Server	Globally
Performance Management – Application	BMC AppSight	FABS
Performance Management – Application	CA Wily Introscope	FABS
Performance Management – Application	LoadRunner	FABS
Performance Management – Application	EWM - > Open View Support Centre	HP
Performance Management - Monitoring	BMC PATROL	LCMG
Performance Management - Network Performance	Packeteer	FABS
Performance Management - Network Performance	IxChariot	Global Crossing
Performance Management - Trend Analysis	Mtracking	MCS

Performance Management - Trend Analysis	WebTrends	MCS
Policy Management	McAfee ePolicy Orchestrator (ePO)	Globally
Policy Management - Log analysis	BT Log Analyser	LCMG

There is also Site Confidence – a web performance and availability tool



**Figure 6 - Service Management processes**

Figure 6 show an overview of the ITIL service management processes. Where tools already exist, they are highlighted in green.

## 5.3 Physical Domain Model

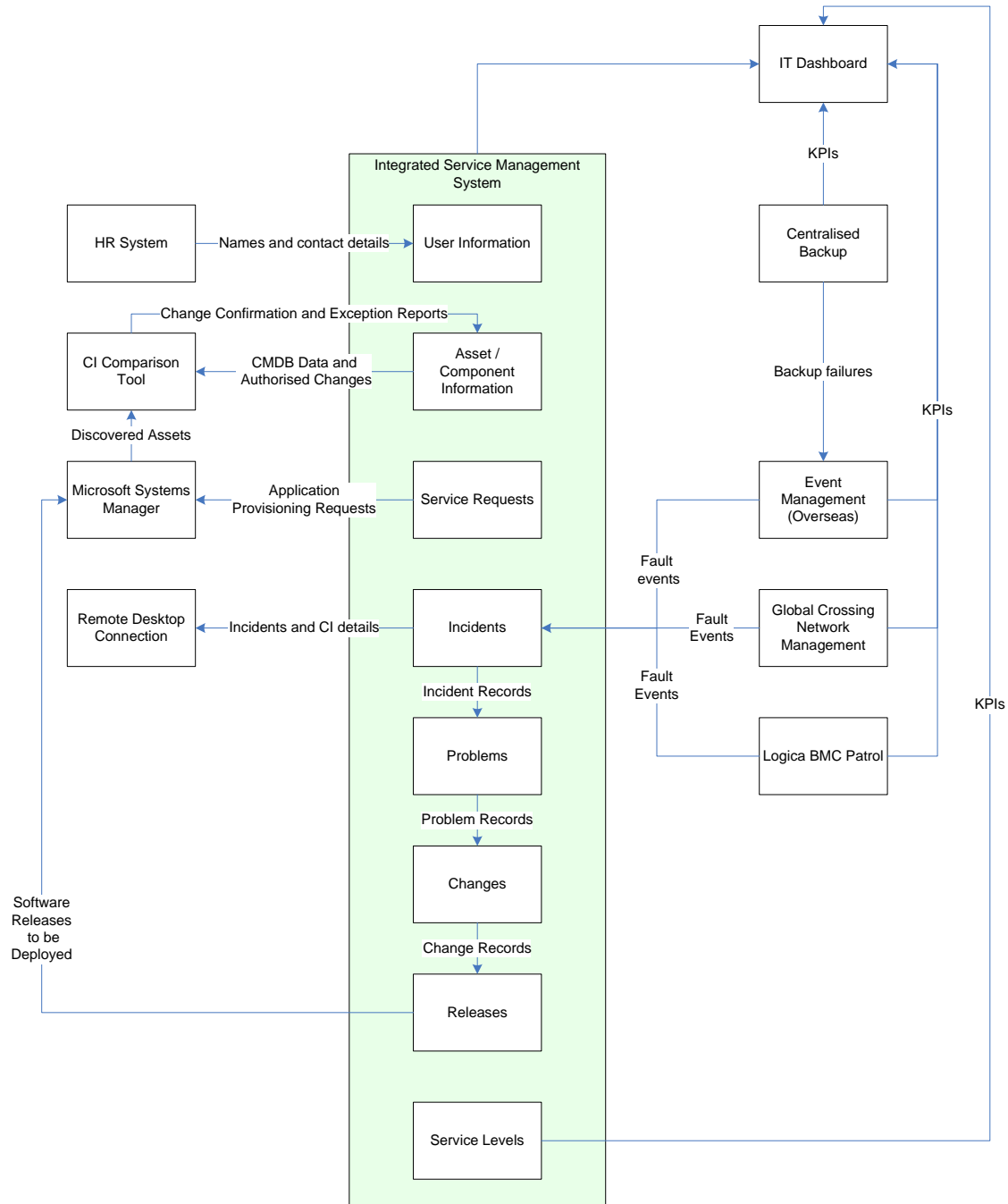


Figure 7 - Physical Domain Model

Figure 7 illustrates how system management tools would integrate with a central integrated *service management* system.

## **6.0 Making it Happen**

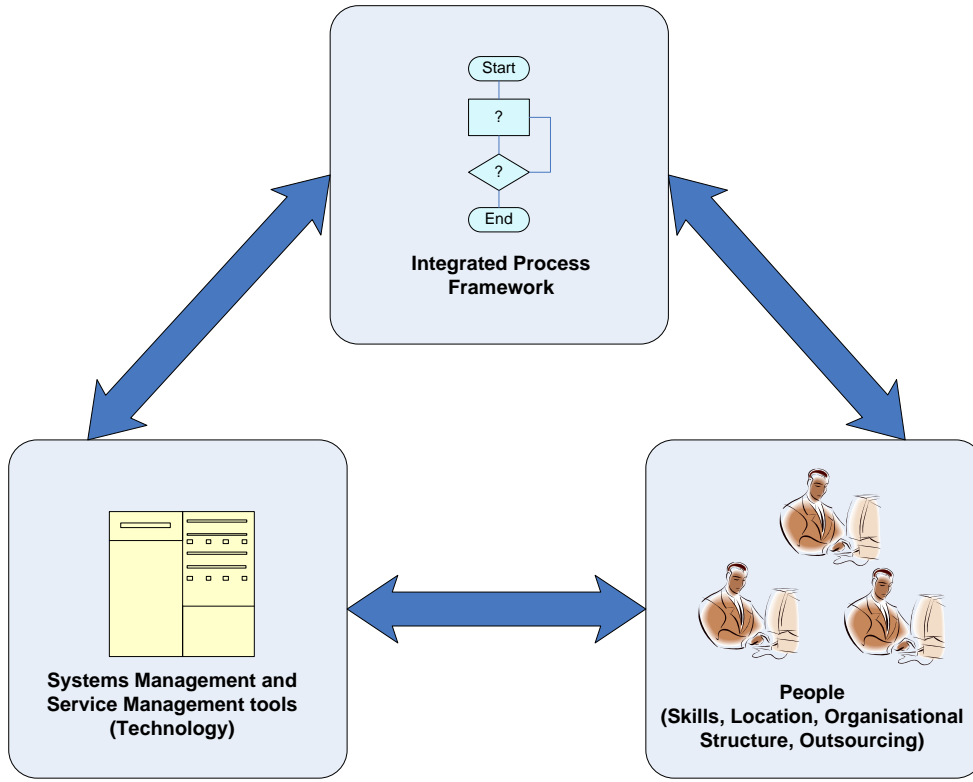
### **6.1 Technology Choices**

The British Council has, and under current plans will continue to have, a large section of its IT infrastructure that is not managed by a third party. That infrastructure resides overseas. The Council will need to implement all of the above Systems Management capabilities to ensure operational stability of that infrastructure.

The British Council has invested heavily in Microsoft-based infrastructure and so the natural first choice of tactical platform-level systems management tools would be the relevant Microsoft offerings, such as SMS, the Systems Center suite, etc. The choice of higher-level integrated suites is best left until the Service Management strategy has been confirmed.

### **6.2 Key Organisation Processes**

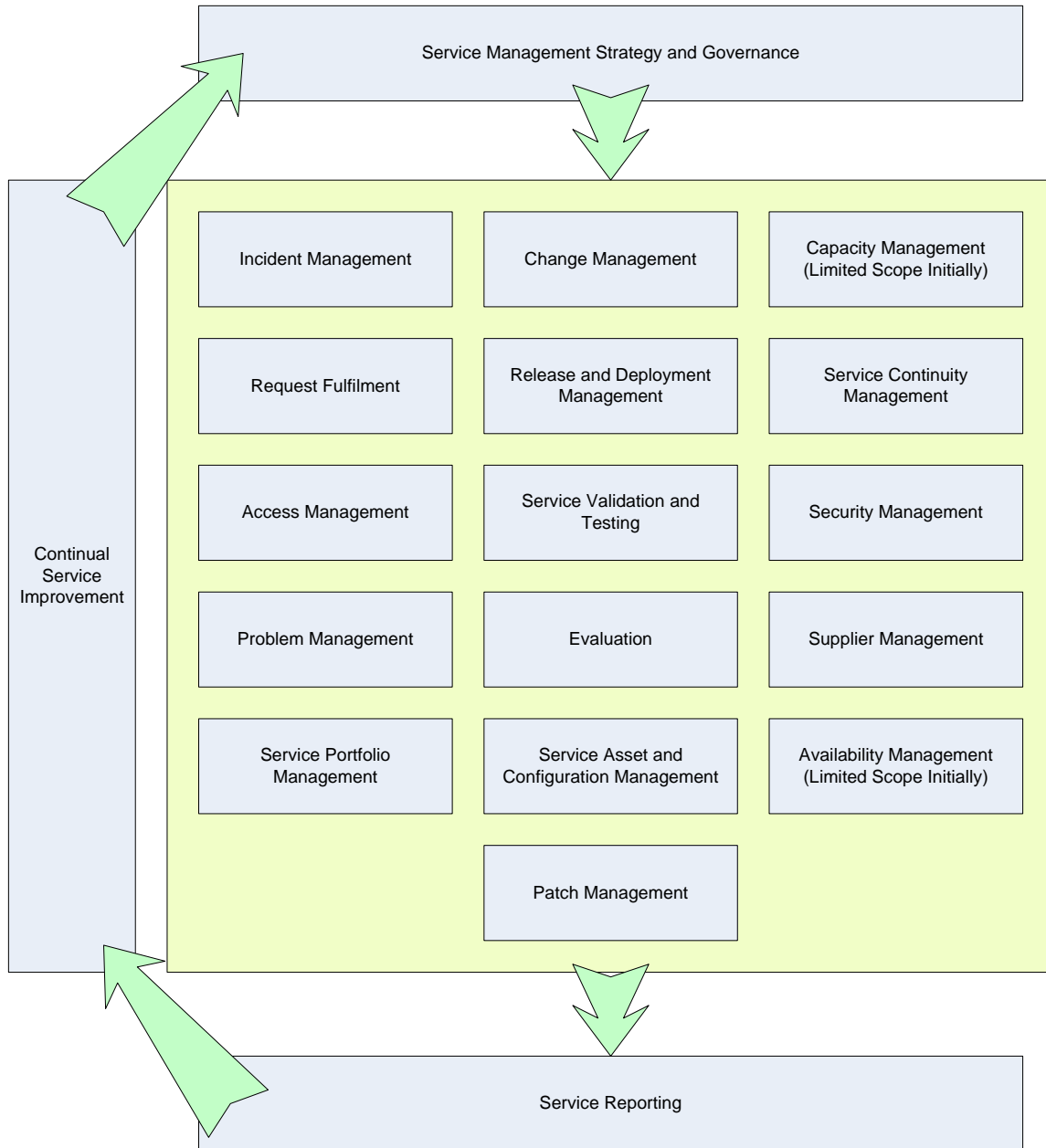
In order to realise the true benefits from investment in Service and Systems Management tools it is essential to realise that the tools are only one part of the required solution. The tools are actually there to facilitate and automate the IT processes required to ensure that IT services are delivered to the business consistently and in accordance with business requirements.



**Figure 8 - People, Process and Product**

To operate the processes and tools, there also needs to be an appropriate staffing model, which provides the necessary headcount, skills and structure.

The processes recommended for inclusion within the process framework are shown in the diagram below:



**Figure 9 - Systems Management Process Framework**

Each of the processes is briefly described below:

- Service Management Strategy and Governance
  - Process focused on the overall ownership and governance of the Service Management strategy, process framework and supporting tools
- Service Reporting

- Design, implementation and operation of required reporting capabilities, both for individual processes and overall Service Management governance
- Continual Service Improvement
  - Process concerned with the identification, justification and management of improvements both to processes and IT services
- Incident Management
  - Process responsible for managing the lifecycle of all incidents
- Request Fulfilment
  - Process responsible for managing the lifecycle of all service requests.
- Access Management
  - Process responsible for allowing users to make use of IT service, data or other assets. Sometimes referred to as Identity Management.
- Problem Management
  - Process responsible for managing the lifecycle of all problems
- Service Portfolio Management
  - Process concerned with managing the Service Portfolio, which includes planned, current and retired services. This includes assessing which proposed services should be designed and implemented
- Change Management
  - Process concerned with managing the lifecycle of all changes
- Release and Deployment Management
  - Process responsible for planning, managing and deploying releases. Releases may be hardware, software or a combination of different CI types
- Service Validation and Testing
  - Process that validates and tests that new or changed services match their design specification, meet any defined acceptance criteria and meet the needs of the business
- Evaluation
  - Process for evaluating proposed solutions or changes to ensure that specified criteria (such as architectural principals, standards and policies) are met and that any risks have been identified
- Service Asset and Configuration Management
  - Process responsible for identifying and managing both asset and configuration information
- Patch Management
  - A sub-process within Release and Deployment Management, concerned with the identification, analysis, testing and deployment of relevant patches (typically security patches) within timescales appropriate to the criticality of the patch
- Capacity Management
  - Process responsible for ensuring the capacity of IT components, services and infrastructure, supports the delivery of agreed service levels in a timely and cost efficient manner
- Service Continuity Management
  - Process responsible for underpinning wider Business Continuity Management, by managing the risks that may cause a serious impact to the delivery of IT services
- Security Management
  - Process focused on maintaining the confidentiality, integrity and availability of the organisation's assets, including information, systems and components
- Supplier Management

- Process concerned with managing the relationship with suppliers including outsourced service providers. Responsible for monitoring contractual compliance including the meeting of agreed service levels
- Availability Management
  - Process responsible for designing, analysing, planning, measuring and improving service availability levels, in accordance with business requirements

### **6.3 Resources and Skills**

Outsourcing of responsibility shifts the balance of skills needed in-house, with a greater emphasis being placed on Supplier Management.

However, the British Council has, and based on current understanding will continue to have, a large section of its IT infrastructure that is not managed by a third party. This overseas infrastructure plays an equally important part of the British Council's business, in most cases forming part of the end-to-end service delivery pathway alongside those elements that are managed by a third party. Therefore, each of the processes outlined in section 6.2 above will need to be staffed appropriately.

### **6.4 Provision Assumptions**

Ultimately, this will depend on any decision to outsource the overseas platform. Assuming that an outsourcing model is applied:

- Outsource system management
- Keep senior architects in-house for ensuring that system management components across multiple services are effectively integrated
- Service management tools are managed in-house

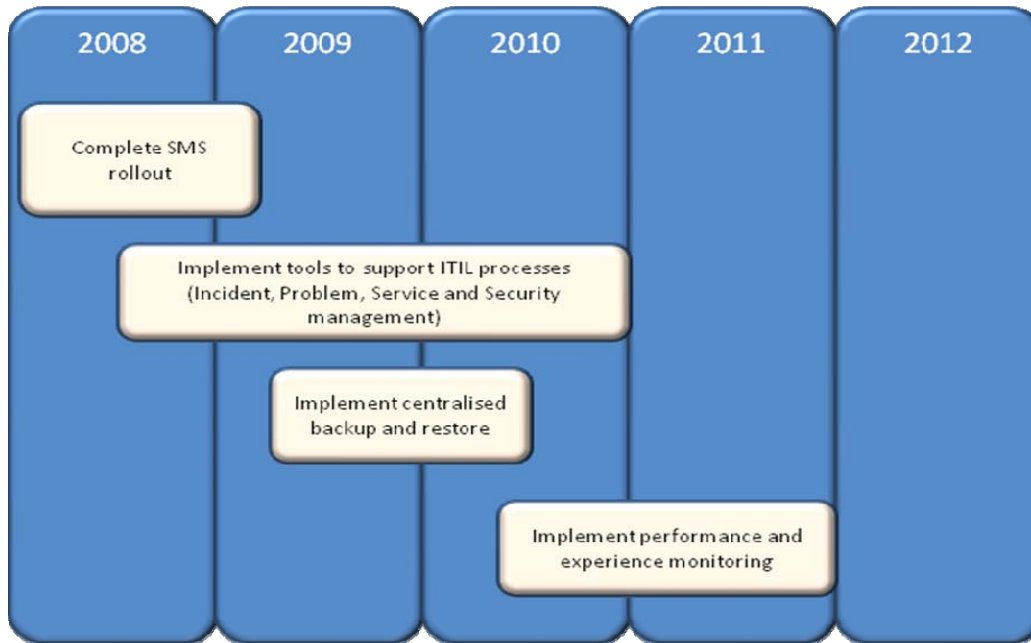
Alternatives:

- Outsource service management to 3<sup>rd</sup> party
- Keep senior architects in-house to oversee supplier management processes and tools

### **6.5 Milestones and Deadlines**

The roadmap for implementation of the Systems Management Domain is linked to the *Service Management* roadmap and also any decision on outsourcing of the overseas platform.

## 6.6 Domain Strategic Roadmap



**Figure 10- Platform Domain High-Level Strategic Roadmap**

### 6.6.1 Step 1 – Complete SMS rollout

The first step is to complete the current program of rolling out SMS. See section 4.5.1

### 6.6.2 Step 2 – Implement integrated tools to support key ITIL processes

Four key service management processes have been identified:

- Incident management
- Problem management
- Service management
- Security management

While some limited tool support exists for these processes where defined, the recommended approach is to move to an integrated service management toolset. See section 4.5.2

The priority should be:

1. Implement tools where they do not already exist, ensuring that all new tools are part of an integrated systems management toolset architecture
2. Integrate existing tools over time (or migrate to integrated tools as replacement)

### 6.6.3 Step 3 – Implement Centralised Backup and Restore

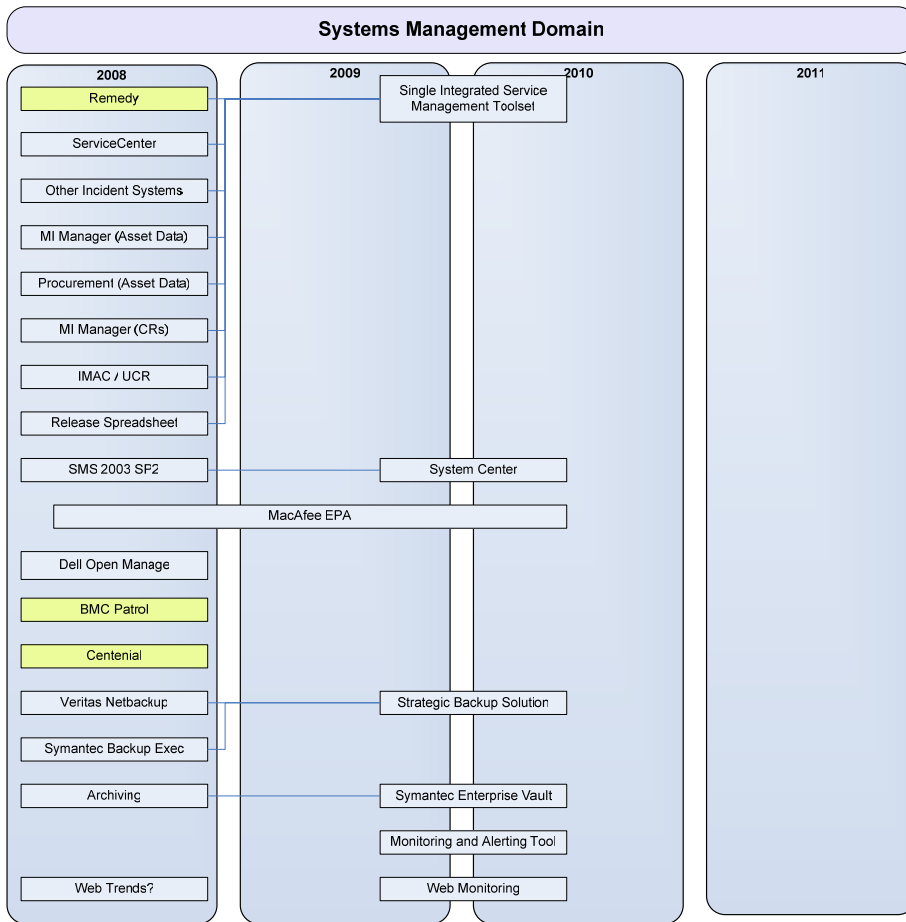
Centralised backup and restore can return significant benefits in terms of reduced operation cost and improved availability management.

Some work has already been done to develop a business cases, and this should continue. See section 4.5.3

### 6.6.4 Step 4 – Implement Performance and Experience Monitoring

In the slightly longer term, additional benefits can be realised by improving the performance and experience monitoring capabilities. Tools to support this should be synchronised with the implementation of the availability management process. See section 4.5.3

## 6.7 Domain Technical Roadmap



**Figure 11 - Domain Technical Roadmap**

Figure 11 - Domain Technical Roadmap above will need to be refined further as the Systems Management Platform domain roadmap is finalised.

## **7.0 Appendix 1 – Principles Guiding the Systems Management Domain**

### **7.1 Business Principles**

Business Principle 1 - Climate Change and Environmental Policy  
Business Principle 2 - Business Agility  
Business Principle 3 - Maximising Efficiency  
Business Principle 5 – Security Strategy

### **7.2 Functional Principles**

Functional Principle 2 – Modular Solutions  
Functional Principle 3 - Scalability and performance  
Functional Principle 4- Legal and Regulatory Requirements  
Functional Principle 5 – Confidentiality, Integrity and Availability of Data and Systems  
Functional Principle 6 – Security Policy  
Functional Principle 8 – Business Continuity

### **7.3 Technical Principles**

Technical Principle 2 – Maximising Microsoft Infrastructure Benefits  
Technical Principle 3 - Industry Standards  
Technical Principle 4 - Buy not build  
Technical Principle 5 - Flexibility  
Technical Principle 6 - Non-vendor specific solutions  
Technical Principle 7 – Security Standards  
Technical Principle 10 - Solution Characteristics  
Technical Principle 11 - Systems Management

### **7.4 Implementation Principles**

Implementation Principle 1 – Health & Safety  
Implementation Principle 2 - Strategic Suppliers and the British Council  
Implementation Principle 3 - Provision of Services

### **7.5 Governance Principles**

Governance Principle 1 - Enterprise architecture is business driven  
Governance Principle 2 - Architectural values are to be publicised  
Governance Principle 3 - Architecture efforts must be unified across the Enterprise

## **8.0 Appendix 2 – Systems Management Domain Standards**

For future use: This section will contain a list of systems management specific architecture standards.