FINDINGS PACK

Review of the Transfer of IT Services to the Five Councils Contract

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

HAVANT BOROUGH COUNCIL
PUBLIC SERVICE PLAZA
CIVIC CENTRE ROAD
HAVANT
HAMPSHIRE P09 2AX

Telephone: *023 9247 4174*
Fax: *023 9248 0263*
Website: *www.havant.gov.uk*

2016/17

		Page
A	Introduction	1 - 4
B	Recommendations	5 - 8
C	Conclusions	9 - 12
D	Panel Membership	13 - 16
E	List of Contributors	17 - 20
F	Methodology	21 - 24
G	Questionnaire Sent to Councillors	25 - 28
H	Results of the Councillors' Survey	29 - 34
I	Output Specifications	35 - 86
J	IT Briefing Note	87 - 90
K	Notes of Meetings	91 - 102
L	Scrutiny Project Plan	103 - 110

Introduction

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Introduction

Suffering from unreliable IT systems was identified as the biggest risk in the implementation of the Five Councils Contract.

Our objective was to investigate the implementation plans for outsourcing delivery of IT services for Havant Borough Council to Capita.

All Councillors were consulted and invited to share, via Democratic Services officers, their experiences and concerns regarding the transfer of IT services to Capita. Along with the Panel's comments these concerns were submitted to the IT Client Manager and IT Work Stream Transition Lead for the Five Councils Contract, Mr Craig Richards. Mr Richards was then invited to meet the Panel to discuss these concerns and further questions.

It was pleasing to find that officers had prepared robust specifications and were successfully working with Capita to ensure a seamless transition. The Panel's complete findings are included in this report.

My thanks go to the Officers who provided the fullest answers to Panel's questions and to those Councillors who submitted their concerns and comments on the transfer. Councillor Tim Pike led this review as previous Scrutiny Lead and our thanks go to him for his diligence and insight along with the other members of the Panel.

Signed by Councillor Lance Quantrill
January 2017

This page is intentionally left blank

Recommendations

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

RECOMMENDATION

That the findings of the report be noted.

This page is intentionally left blank

Conclusions

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

CONCLUSIONS

For a successful transfer of IT systems to Capita, a robust and sustainable specification and business plan is required to ensure a smooth transfer of the Council's IT systems from the current provider to Capita.

A survey of Councillor found a number of concerns relating to security, access by Councillors and the impact on services, customers and councillors.

The review examined the service specifications for the IT transfer and discussed the implementation of the contract and the concerns raised by councillors with the IT Client manager and IT Work Stream Transition lead.

The Panel was assured that concerns raised by councillors would be addressed and sufficient training given to all users at the beginning of the contract.

The Panel was also advised that the Council would benefit from the lessons learnt in transferring the IT systems of the other participating in the Five Council's contract.

There was clear evidence that the procedures and specification are robust and should enable as smooth as possible transfer of the IT systems to Capita with a minimum disruption to the Council's services and public.

This page is intentionally left blank

Panel Membership

Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

Scrutiny Lead:

Councillor Pike

Panel Members:

Councillors Pike, Shimbart, E Shimbart, Blackett, Quantrill and Kerrin

Cabinet Lead:

Councillor Bains (Cabinet Lead for Marketing, Business Development and Five Councils)

The attendance record for meetings of the Panel is shown below:

Attendance Records – Panel Members

Councillor	Total Expected Attendances	Present as Expected	Absences (Inc Apologies)
Councillor Mrs Blackett	2	2	0
Councillor Kerrin	2	0	2
Councillor Pike	2	2	0
Councillor Quantrill	2	0	2
Councillor Shimbart	2	2	0
Councillor Mrs Shimbart	2	1	1
Councillor Bains	2	2	0
Councillor Branson	2	2	0
Councillor Francis	2	0	0
Councillor Ponsonby	2	2	0
Councillor Wade	2	2	0
Councillor Buckley	2	1	0

Attendance Record – Guests

Councillor	Total Attendances
Councillor Branson	2
Councillor Francis	0
Councillor Ponsonby	2
Councillor Wade	2

Attendance Record – Cabinet Lead

Councillor	Total Attendances
Councillor Bains	2

Attendance Record – Scrutiny Board Chairman

Councillor	Total Attendances
Councillor Buckley	1

List of Contributors

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Contributors to the Review

Who?	Contribution	When?
Craig Richards, It Client manager & IT Work Stream Transition Lead	Provided documentation and met with the Panel to discuss the transfer of IT to Capita	Throughout the Review
Susan Parker, Head of Programmes, Redesign and Quality	Provided advice on the scope of the review	26 September 2016
Dawn Adey, Transition and Transformation Lead	Met with the Panel to discuss the transfer of IT to Capita	6 December 2016

This page is intentionally left blank

Methodology

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Scope

To understand the implementation plans for the transfer of the IT systems to Capita.

Links with the Corporate Strategy and Business Plans

The Council is committed to public service excellence and the IT systems for officers are a fundamental part of delivering all Council services. The Council is also committed to looking at innovative and creative ways to deliver services and the 5 Councils Contract is a leading example of commissioning external companies to deliver a number of services within the Council.

Benefits to the Council and Its Residents

The Council will greatly benefit from a smooth transition to the new IT systems and this will in turn benefit residents

Evidence to Support the Project

IT has been identified as the major risk of the Five Councils Contract.

The Project Included

1. A survey of HBC Councillors to ascertain their concerns over the transfer of IT under the 5 Council's contract.

2. Interview with a IT Client manager & Work Stream Transition Lead – 5 Councils Partnership.

This page is intentionally left blank

Questionnaire Sent to Councillors

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Questionnaire Sent to HBC Councillors

The Marketing and Development Scrutiny Panel are receiving updates on the progress of the 5 Councils Contract and the implementation at HBC. One element that has been identified as an area of concern for members is the transfer of IT systems to Capita.

Please can we request that you complete the below questionnaire in relation to the transfer of IT systems to Capita. These will inform a meeting with the IT Client Manager, where concerns over the transfer of IT will be discussed.

1. What concerns do you have over the impact of IT systems transferring to Capita on your role as a Councillor?

2. What concerns do you have over the impact of IT systems transferring to Capita on the Council's services?

3. If you were a member of the Council when the IT was transferred to Hampshire IT, can you recall any specific issues that were raised during the transfer that you would like to identify as a possible concern for the Capita transfer?

4. Do you have any additional comments or concerns over the IT transfer to Capita?

Please can I ask that any completed questionnaires are sent to me by latest Thursday 13 October. These questions and concerns will then be passed on to the IT Client Manager and his response to these will be made to the Panel. A record of this meeting will be made available to all members.

This page is intentionally left blank

Survey Results

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Councillors' Survey Results

(Transfer of IT to Capita)

Marketing, Business Development and Five Councils Scrutiny Panel

2016

Aim of the Survey

The aim of the survey was to ascertain the concerns of Councillors over the impact of the transfer of the IT systems to Capita

Responses

In total 8 responses were received, achieving a low response rate of 21%

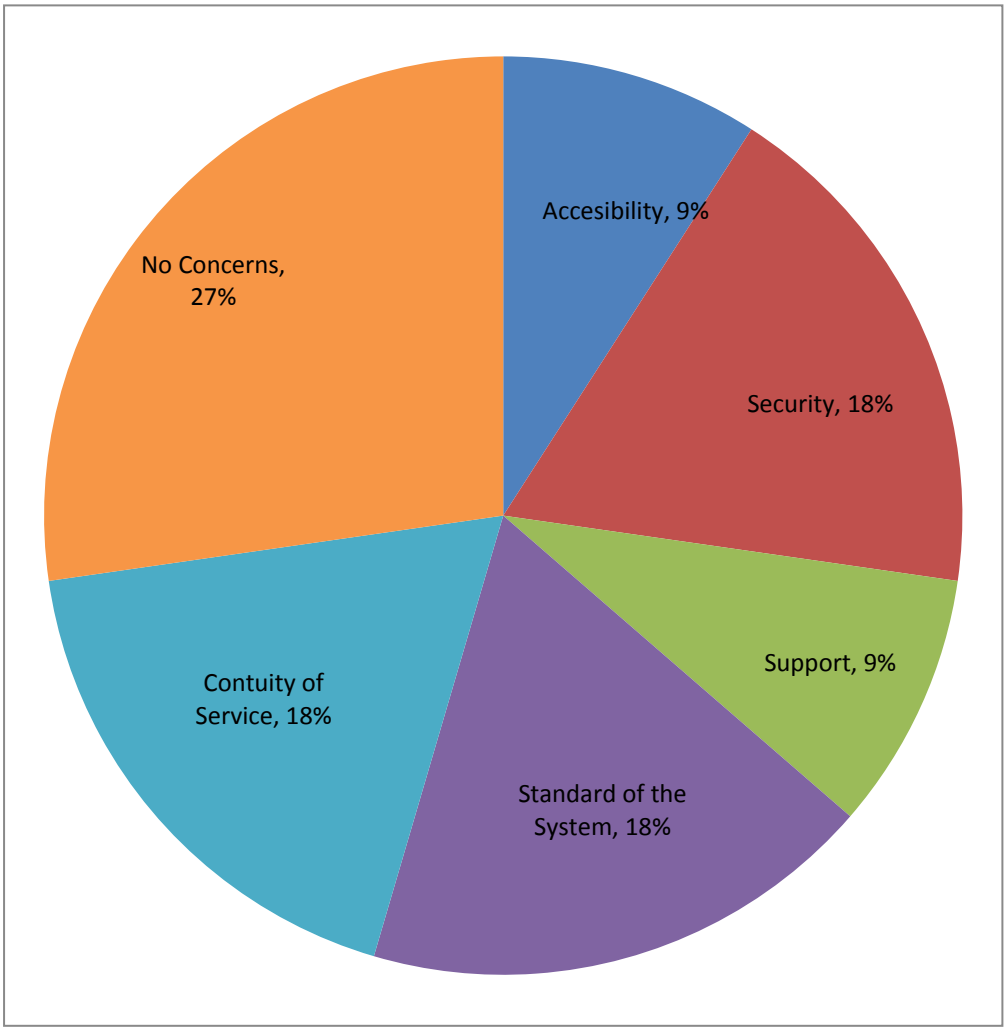
Survey Results

Presentation of findings

In the table and charts that follow, the number of responses analysed are shown as “N”. The number of responses (N) does not always remain the same due to some sections being left blank (no response)

Impact of the Transfer on the Councillor’s Role

Q *What concerns do you have over the impact of IT systems transferring to Capita on your role as a Councillor?*

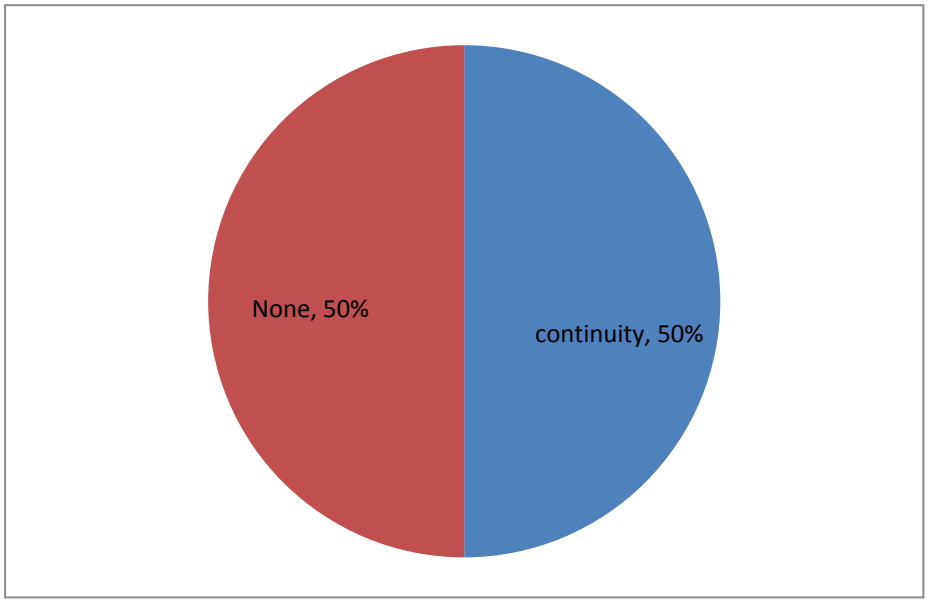


N= 8

Although 28% of the respondents had not concerns, the other respondents raised concerns relating to accessibility, security, support, the standard of the service and continuity.

Impact of the Transfer on Council Services

Q *What concerns do you have over the impact of IT systems transferring to Capita on the Council's services?*

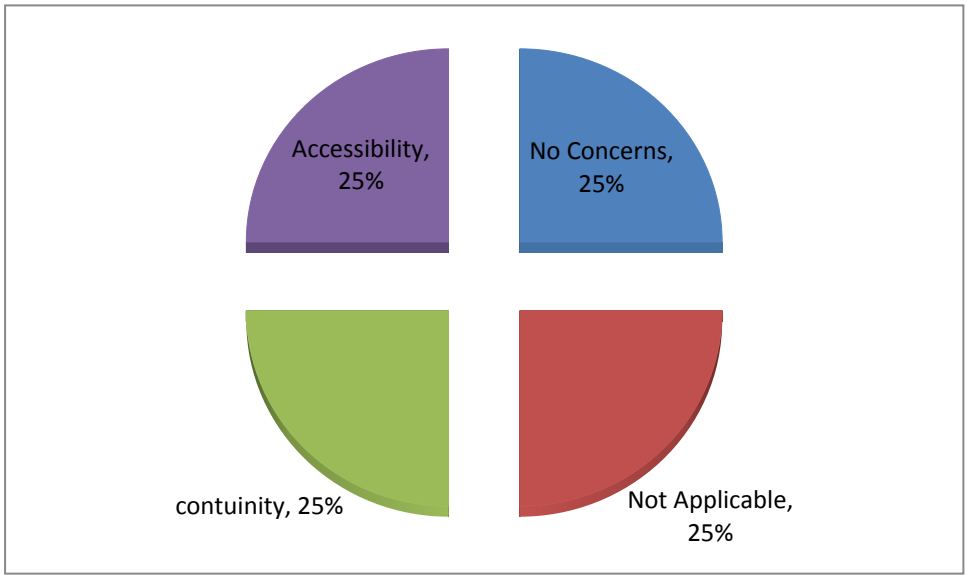


N= 4

Whilst 50% of the respondents had no concerns the remainder were concerned about continuity.

Specific Issues

Q *If you were a member of the Council when the IT was transferred to Hampshire IT, can you recall any specific issues that were raised during the transfer that you would like to identify as a possible concern for the Capita transfer?*

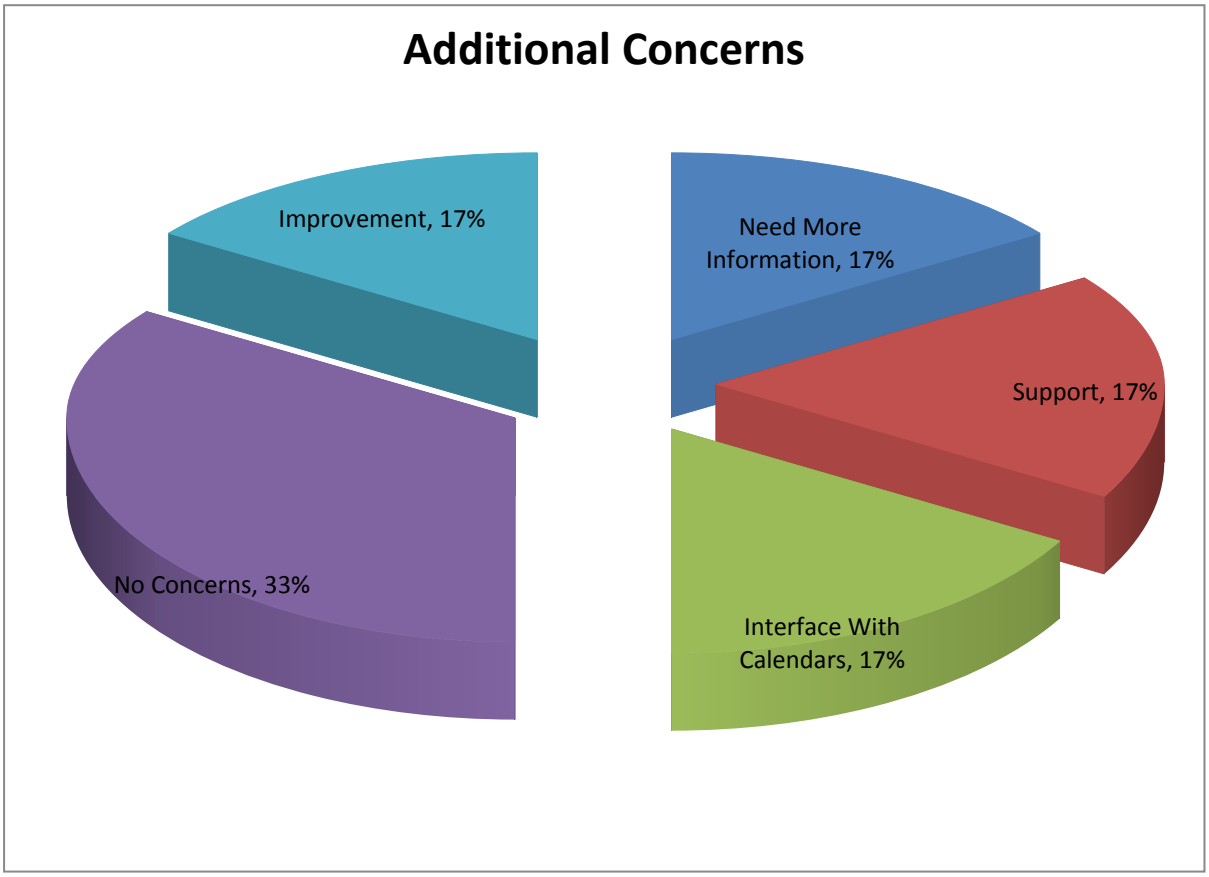


N=4

A quarter of the respondents were unable to answer because they had not experienced the transfer to Hampshire IT. Another quarter of the respondents had not concerns. The remaining 50% of the respondents identified the issues of accessibility and continuity.

Additional Comments and Concerns

Q Do you have any additional comments or concerns over the IT transfer to Capita?



N= 6

49% either had no concerns or need more information before they could comment. The remainder raised the issues on improvement to the current service, the need to interface with private calendars and the level of support.

Output Specifications

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Five Districts Corporate Services Project

Service Specification:

IT Operations System/Applications Support

Contents

Introduction 3
Scope 4
Service Requirements 5
Definitions and Glossary 13

Introduction

This service specification represents the requirements of Hart District Council, Havant Borough Council, Mendip District Council, South Oxfordshire District Council and Vale of White Horse District Council, hereafter known as the Authorities.

In developing their requirements the Authorities have recognised that the expectations of service users, and the financial, technological and legislative environment in which the Authorities operate will change. The Authorities expect their partner(s) to deliver best in class performance throughout the Term of the Agreement and this is expressed in terms of:

(i) Delivering the individual service requirements as specified for all Authorities

(ii) Supporting the delivery of corporate outcomes common to all of the Authorities that cut across one or more of the services in the scope of this partnership

(iii) Delivering specific outputs and outcomes for individual Authorities

For the avoidance of doubt it should be assumed that such delivery will be in accordance with all prevailing legislation and generally accepted codes of practice from relevant bodies such as CIPFA, IRRV etc.(unless specifically highlighted otherwise).

Scope

The following functions are included within the scope of this service:

IT Applications and Systems support

Service Component	Hart	Havant	Mendip	South Ox	Vale
Change Management	x	x	x	x	x
Software Installation & Support	x	x	x	x	x
Database administration		x	x	x	x
Servicedesk calls & requests	x	x	x	x	x
Release Management	x	x	x	x	x
Training				x	x
Systems backup and Disaster Recovery	x	x	x	x	x
Systems management	x	x	x	x	x
Telephone system administration & support		x	x	x	x
Support of in-house developed applications				x	x

Service Requirements

The service specific requirements of the Authorities are as follows:

REF	Service Component	Requirement	Frequency / Volumes
IT301	Change Management	The Supplier shall: • Implement an agreed change management process, emergency change request and impact analysis of proposed changes • Establish a forward schedule of change in conjunction with the Authorities • Undertake configuration changes for general release or Commercial off-the shelf (COTS) operating systems and applications supported by the Supplier • Where agreed as part of the change request, the Supplier will ensure where possible all changes are tested within a test environment • Ensure that prior to installing any changes a documented back-out plan is recorded including any restorable backups exist for the system being changed Incorporate references against a configuration record database (CRD) Define and agree how planned outages will be managed	
IT302	Software Installation and support	Supplier to deliver installation and support services to a range of corporate applications. Applications includes but not limited to • Oracle client and, reports and forms • Ocella suite of applications • Council GIS • cash receipting eg Civica Icon, PARIS etc • WEB content management – eg Drupal, Joomla, iGOSS	

REF	Service Component	Requirement	Frequency / Volumes
		• OpenHR • Anite@work • Xpress elections • Civica IBS • Microsoft Office Suite – 365 and on premise applications, • Chipside – parking • EMC Legato • Sophos anti virus • MapInfo Professional • ExeGesIS • iShareMaps • iShareGIS • Agresso • Axis/AIM • Sharepoint – hosted and on-premise Supplier to work with suppliers and 3rd party maintainers of corporate applications to deliver support to Authorities' end-users Supplier to provide support to support to 3rd party browser based software accessed either directly or via remotely hosted citrix sessions. Supplier to ensure desktop environment is configured which correct applications for end users and Authorities' service teams to be able to complete their business tasks. Supplier to manage and deploy software patches and application updates in line with recommendations from manufacturers, system suppliers or IT security team.	
IT303	Database	Supplier to deliver database management and administration to the Authorities'	

REF	Service Component	Requirement	Frequency / Volumes
	management and administration	databases. Oracle • Ocella suite of applications • Servicedesk • Swift licencing • Inhouse Oracle databases • Symphony • Ebase • Uniform MS SQL • TF property maintenance • Icon Cash Receipting • Iken legal case management • InCase fraud management • OpenHR • Xpress • Chipside • M3 Public Protection MYSQL • Drupal CMS - for council websites • Joomla CMS - for councils intranet Progress Civica IBS PostGreSQL To monitor performance of databases and proactively manage issues before they have operational impact.	

REF	Service Component	Requirement	Frequency / Volumes
		Upgrade and patch all database systems in line with supplier, manufacturer or IT security requests. Test upgrades and migrations before implementing into live environment. Work with in-house/3rd party development team on database changes.	
IT304	Servicedesk calls and requests	Supplier to deliver 2nd and 3rd line support for applications, databases and systems support for all services under corporate contract. To complete all calls and requests within Authorities' SLA's. SLA to be in accordance with those defined in Service desk specification	Approx. 2900 incidents and service requests per annum Hart approx. 876 incidents logged each year 708 resolved by level 2 116 resolved by level 3 28 by infrastructure 24 security Approx. 550 change requests per annum Hart Approx. 236 change requests per annum
IT305	Release Management	The Supplier shall: • Establish a formal sign off for release procedures to include design, build, roll-out, purchasing, installing, moving and controlling software and hardware • Establish a release acceptance procedure • Clearly define and agree ownership of processes and responsibility for	

REF	Service Component	Requirement	Frequency / Volumes
		service delivery • Provide release policy and procedures to ensure that changes to the live production environment are effected in a controlled manner. • Provide appropriate mechanisms and procedures to address media requirements, naming conventions, build management, testing and back out plans, security and audit plans • Establish testing procedures • Ensure the CRD is updated User Acceptance testing to be signed off before release is implemented into a live or production environment.	
IT306	Training	Supplier to deliver end user training on range of corporate applications developed by in-house software team – South Oxfordshire & Vale of White Horse district councils. • GIS • eForms applications eg recruitment • Java applications • Oracle forms or reports Provide end user training notes and/or documentation to complement training sessions	
IT307	Systems backup and Disaster Recovery	Supplier to deliver system, application and data backups on an agreed schedule to maintain integrity to Authorities' systems Supplier to deliver system, application and file restore services to maintain operational availability of data. Supplier to monitor and document backups to provide evidence of successful	

REF	Service Component	Requirement	Frequency / Volumes
		backups. Supplier will record and investigate any failed backups and resolve within agreed timescales. A suitable backup regime for recovery of historical data for a 6 month period should be delivered. Backup data to be kept away from data-centres and available 24x7 for recovery or restore processes. Supplier to test annually the recovery of applications and systems; to evidence applications can be recovered from a backup. Written report confirming tests and results of testing to be delivered to the Authorities' Representative Disaster Recovery. Testing: Supplier to supply annual test of DR plans for each Authority, working with any 3rd party specialist appointed by the Authorities as necessary. Document DR testing and update plans accordingly. Record and investigate any failed DR tests and resolve within agreed timescales. Evidence each councils applications can be recovered in line with each Authorities' business continuity plan. Invocation: Supplier to assist the councils when invoking a DR plan. To work with any Authorities' 3rd party DR specialists and to provide onsite resource to meet the Authorities' recovery. Supplier to deliver IT resources needed to execute each Authority DR plan and assist in the Authorities' business continuity plans.	

REF	Service Component	Requirement	Frequency / Volumes
IT308	Systems management	Supplier to deliver performance and management of corporate applications. Monitor performance of applications to prevent issues having operational impact. Recommend updates or changes to ensure applications run within user acceptable tolerance. Forward planning of changes and upgrades to applications. To have an agreed plan up updates or upgrades Applications and systems to current and/or supported version as defined by manufacturer/supplier. To work with suppliers of applications used by Authorities to agree scheduled updates and migrations. Update services will be provided for business applications supported by third party support providers	
IT309	Telephone system administration and support	Supplier to deliver first line support of Authorities' telephone systems. To provide changes and updates to telephone systems requested by end-users authorised by service or change requests. Including programming system, updating system voicemail messages, setting up hunt and pickup groups To work with authorised 3rd party maintenance suppliers to: • Install hardware or software updates • resolve system problems • implement new feature or upgrades Updating call logger with tariff information, person or departmental changes, or other information to ensure telephony reporting is accurate and relevant. Provide monthly reporting on telephone usage, create reports in call logger.	

REF	Service Component	Requirement	Frequency / Volumes
IT310	Support of in-house developed software	Supplier to work with in-house software development team to support installation and support of applications and reports. Supplier to support in-house developed applications, for example Java applications or Oracle based reports. Service desk Some service and change requests will be marked for in-house IT Development team (South Oxfordshire & Vale of White Horse). Some activities and actions within these requests will be delivered by the IT applications team. Supplier to make sure these are actioned in a timely manner to keep IT Development projects on track. Supplier to work with any in-house IT development team to deliver application testing for in-house developed software. Software application testing to be delivered against agreed testing methods and specification agreed by end-users. Supplier to deliver documentation for end-users for using applications developed by in-house IT Development team - South Oxfordshire & Vale of White Horse.	

Definitions and Glossary

(to be completed when all Councils have inputted into the requirements. This is intended to provide a glossary for acronyms, Council specific applications or processes etc.)

Term	Definition
ITIL	IT Infrastructure Library
CRD	Change release document
DR	Disaster Recovery
BC	Business Continuity

This page is intentionally left blank

Five Districts Corporate Services Project

Service Specification:

IT Operations Infrastructure Support

Contents

Introduction 3
Scope 3
Service Requirements 4
Definitions and Glossary 11

Introduction

This service specification represents the requirements of Hart District Council, Havant Borough Council, Mendip District Council, South Oxfordshire District Council and Vale of White Horse District Council, hereafter known as the Authorities.

In developing their requirements the Authorities have recognised that the expectations of service users, and the financial, technological and legislative environment in which the Authorities operate will change. The Authorities expect their partner(s) to deliver best in class performance throughout the Term of the Agreement and this is expressed in terms of:

(i) Delivering the individual service requirements as specified for all Authorities

(ii) Supporting the delivery of corporate outcomes common to all of the Authorities that cut across one or more of the services in the scope of this partnership

(iii) Delivering specific outputs and outcomes for individual Authorities

For the avoidance of doubt it should be assumed that such delivery will be in accordance with all prevailing legislation and generally accepted codes of practice from relevant bodies such as CIPFA, IRRV etc.(unless specifically highlighted otherwise).

Scope

The following functions are included within the scope of this service:

IT Operations Infrastructure

Service Component	Hart	Havant (including East Hants DC)	Mendip	South Ox	Vale
Hardware Installation & support	X	X	X	X	X
Software Installation & support	X	X	X	X	X
Network Installation & support	X	X	X	X	X
Servicedesk Incident & Request	X	X	X	X	X
Patch Management	X	X	X	X	X
Capacity Management	X	X	X	X	X
Moves, Adds, Deletions & Changes	X	X	X	X	X

Service Requirements

The service specific requirements of the Authorities are as follows:

REF	Service Component	Requirement	Frequency / Volumes
IT201	Hardware installation and support	Supplier to install and support computer hardware including but not limited to • Servers • Storage systems on premise as well as cloud i.e Azure, Amazon AWS Rackspace etc • Desktop PCs • laptops • tablet devices • Thin clients devices • Scanners and printers eg receipt printers • Tapes libraries and associated storage devices e.g. EMC legato • Peripheral devices eg card readers, chip and pin devices • Component devices eg RAM, disk drives, PSU, NICs etc • telephone handsets • mobile handsets • Audio Visual equipment Responding to system alerts raised by hardware systems; Monitor servers and take proactive action to minimise impact or correct issues before they develop into operational problems. Supplier to ensure desktop environment is suitable to meet the needs of the end-user and service area. Each desktop environment should • boot up and allow the user to logon to the network within 30 seconds	

REF	Service Component	Requirement	Frequency / Volumes
		• be responsive to user requests via keyboard and mouse. • Be functional and provide all the software and network access a user needs to complete their work • Be flexible to allow for changes in working patterns and environments used by the Authorities. Not to be hindered by the lack of appropriate IT resources Supplier to support Authority owned hardware devices either via third party maintenance or directly if no external maintenance contract is in place. Supplier to have suitable hardware warranty or maintenance agreements for core infrastructure equipment such as servers, network switches and routers, storage arrays, desktops etc.	
IT202	Software installation and support	Supplier to install and support, where an underpinning agreement with suppliers or manufacturers isn't in place, a range of software systems and applications across the Authorities' networks and service teams. Supplier to have suitable underpinning software and maintenance agreements directly with any software suppliers, for applications delivered by the Supplier. Software includes but not limited to • Server operating systems e.g. Windows, Linux, VMWare, HyperV including cloud based systems like Microsoft Azure, Amazon AWS, Rackspace etc • Anti Virus e.g. Sophos • Backup software e.g.. EMC Legato, Veeam cloud service • VDI - eg VMWare The Supplier will maintain a standard build for all Authorities' desktops, laptops, mobile devices and VDI images. As part of the BAU service the provider will generate a standard build to fit any agreed hardware model Standard build images for desktops, VDI, servers to be built with agreed IT security	

REF	Service Component	Requirement	Frequency / Volumes
		hardening techniques to reflect the nature of the server or desktop environment. Supplier to ensure desktop and server environment is responsive and available to meet the needs of the Authorities' users and service teams. Desktop environment to have the appropriate and correct software to meet the needs of the Authorities' users and service teams so they can undertake their business tasks. Supplier to work with suppliers of Authorities line of business applications to assist in upgrades, fault resolution, migrations or replacements of systems. Supplier to undertake and complete installation and upgrades of line of business applications in line with the Authorities project teams and the project timescales. Supplier to monitor and deploy software patches in line with recommendations from manufacturers or IT security team. Patches and updates includes but not limited to • Desktop operating systems inc laptops and loan laptop equipment • Server operating systems • tablets • Hardware bios updates for servers and desktops • Hardware drivers • Software patches for productivity suites and office applications Supplier to maintain desktop images for VDI solution (Citrix, VMWare etc) Responding to alerts raised by systems; Monitor systems and virtual environments and take proactive action to minimise impact or correct issues before they develop into operational problems.	
IT203	Network installation and support	Supplier to assist in installing and supporting Authorities' network equipment Network switching for Cisco, Extreme Networks and 3COM switches deployed across	

<table>
<tr><th>REF</th><th>Service Component</th><th>Requirement</th><th>Frequency / Volumes</th></tr>
<tr><td></td><td></td><td>Authorities' networks.

Network devices such as switches, routers, firewalls, spam filters, web filters etc

Working with third party suppliers for network switches and WAN to maintain network integrity and service at the following WAN locations:

<table>
<tr><th>Site Name</th><th>Address</th><th>Postcode</th></tr>
<tr><td>Abbey House</td><td>Abbey Close</td><td>OX14 3JE</td></tr>
<tr><td>Civic Offices</td><td>Harlington Way</td><td>GU51 4AE</td></tr>
<tr><td>Havant Borough Council, Public Service Plaza</td><td>Civic Centre Road</td><td>PO9 2AX</td></tr>
<tr><td>Mendip District Council</td><td>Cannards Grave Road</td><td>BA4 5BT</td></tr>
<tr><td>Milton Park</td><td>135 Eastern Avenue</td><td>OX14 4SB</td></tr>
<tr><td>Southmoor Depot & Offices</td><td>2 Penner Road</td><td>PO9 1QH</td></tr>
<tr><td>Central Beachlands</td><td>7 Seafront</td><td>PO11 0AG</td></tr>
<tr><td>Cornerstone Arts Centre</td><td>25 Station Road</td><td>OX11 7NE</td></tr>
<tr><td>The Beacon</td><td>Portway, OX12 9BX</td><td>OX12 9BX</td></tr>
<tr><td>Audlett Drive</td><td>Audlett Drive</td><td>OX14 3PJ</td></tr>
<tr><td>Abingdon CCTV</td><td>Abingdon Police Station</td><td>OX14 1AU</td></tr>
<tr><td>Foxhall Mobile Home Park</td><td>Basil Hill Road</td><td>OX11 7HJ</td></tr>
<tr><td>Pebble Hill</td><td>Pebble Hill,</td><td>OX14 2JX</td></tr>
<tr><td>Abingdon</td><td>Abingdon</td><td>OX13 3AU</td></tr>
<tr><td>East Hants HQ</td><td>Penns Place, Petersfield</td><td>GU31 4EX</td></tr>
<tr><td>Hampshire County Council Hampshire County Council</td><td>The Castle, Winchester</td><td>SO23 8UJ</td></tr>
</table>

Update and maintain switches, firewalls, routers etc with approved firmware updates.</td><td></td></tr>
</table>

REF	Service Component	Requirement	Frequency / Volumes
		Supplier to diagnose and assist third party suppliers in diagnosing and resolving network issues. Maintain and backup configuration of Authorities' network devices. Provide monitoring and reporting of Authorities' network services. Maintain documentation of network configuration including diagrams, network addressing etc Monitor network and take proactive action to minimise impact or correct issues before they develop into operational problems Manage network resources to ensure suitable bandwidth is available to provide responsive and functional IT environment for the Authorities' users and service teams.	
IT204	Servicedesk incident and requests	Supplier to deliver 2nd and 3rd line support for hardware and software support for all services under corporate contract. To complete all calls and requests within Authorities SLA. SLA and delivery as defined in service desk specification.	Approx 5600 incident and service requests per annum Approx 1350 change requests per annum Hart approx. 876 incidents logged each year 708 resolved by level 2 116 resolved by level 3 28 by infrastructure 24 security Hart – approx. 214 change requests per annum. Hart doesn't split this information out but most would be carried out by 2nd/3rd line

REF	Service Component	Requirement	Frequency / Volumes
IT205	Asset Management	Supplier to maintain software and hardware asset databases when making changes to software or hardware estate. To ensure that asset information is up to date and accurate for the Councils to report on. Supplier to make hardware and software asset database/system available to the client.	
IT206	Capacity Management	The Supplier will monitor and measure system resources to ensure smooth running of network and systems. To prevent predictable events from interfering or degrading networks and systems. Activities to include but no limited to • Monitoring the performance and throughput or load on a server, server farm, or property • Performance analysis of measurement data, including analysis of the impact of new releases on capacity • Performance tuning of activities to ensure the most efficient use of existing infrastructure • Understanding the demands on the service and future plans for workload growth (or shrinkage) • Influences on demand for computing resources • Capacity planning – developing a plan for the service • Report on trends and make recommendations	
IT207	Moves, Adds Deletions, Change (MADC)	The Supplier will undertake all Moves, Adds, Deletions and Changes. MADC relates to an IT activity not related to an incident which will be carried out by a competent engineer. MADC activities will be a response to service or change requests raised and approved via the service desk. Physical MADC services include but not limited to; • Equipment moves for staff relocation or office change • Single equipment installation eg desktop for new starter or installation of	

REF	Service Component	Requirement	Frequency / Volumes
		new printer • Removal of obsolete or upgraded IT equipment from its location to agreed Authorities facility Logical MADC services include but not limited to • BAU changes such as password resets, account administration, access permissions • Application installation • Application removal • Application upgrade • Feature pack install or upgrade • Non-critical patch • Software driver	

Definitions and Glossary

Term	Definition
BAU	Business As Usual – steady state
ITIL	IT Infrastructure Library
MADC	Moves, Adds, Deletions and Changes

This page is intentionally left blank

Five Districts Corporate Services Project

Service Specification:

IT Security

Contents

Introduction 3
Scope 3
Service Requirements 4
Definitions and Glossary 10

Introduction

This service specification represents the requirements of Hart District Council, Havant Borough Council, Mendip District Council, South Oxfordshire District Council and Vale of White Horse District Council, hereafter known as the Authorities.

In developing their requirements the Authorities have recognised that the expectations of service users, and the financial, technological and legislative environment in which the Authorities operate will change. The Authorities expect their partner(s) to deliver best in class performance throughout the Term of the Agreement and this is expressed in terms of:

(i) Delivering the individual service requirements as specified for all Authorities

(ii) Supporting the delivery of corporate outcomes common to all of the Authorities that cut across one or more of the services in the scope of this partnership

(iii) Delivering specific outputs and outcomes for individual Authorities

For the avoidance of doubt it should be assumed that such delivery will be in accordance with all prevailing legislation and generally accepted codes of practice from relevant bodies such as CIPFA, IRRV etc.(unless specifically highlighted otherwise).

Scope

The following functions are included within the scope of this service:

IT Security

Service Component	Hart	Havant	Mendip	South Ox	Vale
IT Security service	X	X	X	X	X
Security Management & Communication	X	X	X	X	X
Software Security	X	X	X	X	X
Hardware Security	X	X	X	X	X
Network Security	X	X	X	X	X
Data Security	X	X	X	X	X
Servicedesk calls and requests	X	X	X	X	X
Security Incidents	X	X	X	X	X
Security Reporting	X	X	X	X	X
Security procedures	X	X	X	X	X
Compliance – PCI-DSS, PSN	X	X	X	X	X

Service Requirements

The service specific requirements of the Authorities are as follows:

<table>
<tr><th>REF</th><th>Service Component</th><th>Requirement</th><th>Frequency / Volumes</th></tr>
<tr><td>IT401</td><td>IT Security service</td><td>The Supplier will provide security device administration and support services for the Authorities' security devices and services

The Supplier will be responsible for operating the client security policy through the maintenance of security configurations enforcing that policy.

The scope of responsibility between the Supplier and the Authorities for security management is detailed within the table below

<table>
<tr><th>Administration Item</th><th>Summary</th><th>Supplier</th><th>Authority</th></tr>
<tr><td>Security Policy</td><td>Define a security policy to maintain a secure environment for hosted applications, network access control and the network</td><td></td><td>✓</td></tr>
<tr><td>Policy Changes Authorisation</td><td>Identify nominated contacts that may submit application configuration changes that impact either directly or indirectly on the security policy</td><td></td><td>✓</td></tr>
<tr><td>Software Patch Updates</td><td>Monitoring of security vendor web site for critical patches, patches to be applied according to security policy. Non-critical patches only implemented where relevant.</td><td>✓</td><td></td></tr>
<tr><td>Software Fault</td><td>Software fault support to resolve any event impacting on the operation of the security</td><td></td><td></td></tr>
</table>
</td><td></td></tr>
</table>

REF	Service Component	Requirement				Frequency / Volumes
		Support	device, including errors in configuration by the Supplier	✓		
		Software Administration	Manage all agreed security policy rules within service levels; implement security policy changed under an agreed change management procedure.	✓		
		System Platform Configuration	Maintain a secure configuration of the hardware platform and its operating system, implementing any security enhancements as and when published by the vendors	✓		
		Web Management (URL access security)	Modify policy if approved change requested, review URL access reports and notify the councils of serious attempted policy breaches e.g. multiple access attempts to web site with extremely unacceptable material.	✓		
		Third Party Access	Approve access requests submitted through the change management process for 3rd parties utilised by the Authorities outside the scope of the Supplier agreement with the Authorities		✓	
		Passive Security Monitoring	Monitor application services to record any logged attempted policy breaches.	✓		
		Active Security Monitoring	Monitor security events as alert events occur and where security device configuration does not apply e.g. internal security breach.	✓		

REF	Service Component	Requirement	Frequency / Volumes
IT402	IT Security Management and communication	The Supplier will provide IT security management services Security system configurations must be aligned to the Authorities' IT security policies e.g. • IT security policy • Remote access policy • Removable media policy etc In absence of such policies or information any such systems will be configured with default security parameters only and as such the Supplier cannot ensure the security systems will operate in line with business operational practices Supplier will hold scheduled service delivery reviews and will report on attempted breaches against the security policies. Supplier will notify the Authorities immediately of any serious breach of the Authorities' IT security policies All other incidents and breaches to the IT security policy must be reported at the next review meeting. Review to provide • impact of breach • actions taken to control breach • actions to stop further occurrences	
IT403	Software Security	Supplier to monitor and check software patching to ensure software is kept up to date to minimise the potential for vulnerabilities. Work with other IT Infrastructure and Applications teams to implement software patches or upgrades to resolve vulnerabilities. To test and approve default builds on desktops, laptops, tablets, servers, virtual environments for systems hardening to meet best practice, and IT security policies.	

REF	Service Component	Requirement	Frequency / Volumes
IT404	Hardware Security	Supplier to identify issues with hardware which can have implications for IT security. To work with other IT Infrastructure team to deliver hardware updates e.g. BIOS updates or hardware replacement programme to remove vulnerabilities on computer systems, e.g. legacy systems which pose an unacceptable risk.	
IT405	Network Security	Supplier to support and maintain network security. Support, maintain and configure firewalls across Authorities' networks both physical and wireless, including • Maintaining and review firewall rule sets • Configuring changes – VPNs etc • Update firewall software/bios Support, maintain and configure security appliances across Authorities' networks both physical and wireless. • Maintain rule sets • Configuring changes – Vlans etc • Update software/bios Work with IT Infrastructure team to update network equipment to resolve or eliminate vulnerabilities. E.g. Check configuration for routing, rule sets etc.	
IT406	Data Security	Supplier to deliver assistance to minimise or eliminate data loss. Supplier to comply with Authorities data security policies and principles. Supplier to provide advice and good practice support Protect personal data from being sent insecurely or incorrectly	
IT407	Service desk	Supplier to deliver support and requests relating to IT security calls and, service and change	Approx 100 incidents

REF	Service Component	Requirement	Frequency / Volumes
	Calls and requests	requests. All change and service requests to be evaluated on risk and impact, and allocated highest priority. Change and service requests delivered to SLA set out in Service Desk standards	and service requests per annum Approx 100 change requests per annum Hart approx. 24 incidents and service requests per annum Hart approx. change requests per annum. This would be included as part of the overall total of 236
IT408	Security incidents	Supplier to investigate, remediate and document IT security incidents. For example but not limited to • Software virus infections • unauthenticated logins • firewalls alerts • attempted hacks/unauthorised sessions • user breaches - sharing passwords, login details etc All IT Security incidents to be logged as P1 into service desk. Once impact and risk assessed incident can be re-prioritised or change request raised accordingly. Serious IT security breaches to be reported to councils immediately. Log to be kept of each incident with actions taken to remediate or solve.	

REF	Service Component	Requirement	Frequency / Volumes
IT409	IT Security Reporting	Supplier to deliver quarterly reports on IT security issues including • Issues raised by security incidents • Breaches of IT security • current state of IT estate - unpatched systems, unsupported software installations etc • data loss eg laptops, memory sticks Serious incidents to be reported immediately Supplier to monitor log information from firewalls and security appliance to recognise attempts to breach IT security, e.g. hacking attempts, access to control IT systems or services unauthorised access to systems or networks etc	
IT410	IT Security procedures	Supplier to help the Authorities maintain IT security procedures.	
IT411	Compliance	Supplier to maintain systems in accordance with the Authorities' standards to achieve and/or maintain Code of Compliance for PSN and PCI DSS. To provide necessary access to Authorities' systems and networks for Authorities' appointed provider of ITHC, so complete health check report can be delivered Provide advice and support so an active programme is maintained to ensure that all security requirements eg PSN, PCI DSS etc are met prior to any review (annual, quarterly etc) or ITHC. To maintain systems to meet PCI DSS where applicable. To apply, resolve or deploy any remedial actions from ITHC and evidence for PSN. To ensure all actions are completed and reported by deadline for CoCo submissions Provide information and evidence to complete PCI DSS SAQ Assist in completion of PSN Code of Compliance return.	

Page 72

Definitions and Glossary

(to be completed when all Authorities have inputted into the requirements. This is intended to provide a glossary for acronyms, Authority specific applications or processes etc.)

Term	Definition
PSN	Public Services Network as defined by Cabinet Office for secure network between Government Agencies
PCI DSS	Payment Card Industry Data Security Standards
SAQ	Self Assessment Questionnaire
ITHC	IT Health Check – as defined by PSN Code of Compliance
CoCo	PSN Code of Compliance

This page is intentionally left blank

Five Districts Corporate Services Project

Service Specification:

IT Operations Service desk

Contents

Introduction 3
Scope 3
Service Requirements 4
Definitions and Glossary 11

Introduction

This service specification represents the requirements of Hart District Council, Havant Borough Council, Mendip District Council, South Oxfordshire District Council and Vale of White Horse District Council, hereafter known as the Authorities.

In developing their requirements the Authorities have recognised that the expectations of service users, and the financial, technological and legislative environment in which the Councils operate will change. The Authorities expect their partner(s) to deliver best in class performance throughout the Term of the Agreement and this is expressed in terms of:

(i) Delivering the individual service requirements as specified for all Authorities

(ii) Supporting the delivery of corporate outcomes common to all of the Authorities that cut across one or more of the services in the scope of this partnership

(iii) Delivering specific outputs and outcomes for individual Authorities

For the avoidance of doubt it should be assumed that such delivery will be in accordance with all prevailing legislation and generally accepted codes of practice from relevant bodies such as CIPFA, IRRV etc.(unless specifically highlighted otherwise).

Scope

The following functions are included within the scope of this service:

IT Operations Service desk

Service Component	Hart	Havant	Mendip	South Ox	Vale
Service desk recording	X	X	X	X	X
Service desk reporting	X	X	X	X	X
First line support	X	X	X	X	X
Service requests	X	X	X	X	X
Change Requests	X	X	X	X	X
Systems Alert monitoring & management	X	X	X	X	X
Mobile phone management		X	X	X	X

Service Requirements

The service specific requirements of the Authorities are as follows:

REF	Service Component	Requirement	Frequency / Volumes
IT101	Service desk recording and reporting	The Supplier will act as a single point of contact for all IT incidents, service requests and change requests and will manage incidents with 3rd parties through to conclusion The Supplier will record all incidents, service requests and change requests made to the service desk by • phone • email • person • web portal into the service desk system. Calls and requests placed via the web portal to be checked and allocated on the same criteria of those made via phone, in person or email. Co-ordinate second and third line and 3rd party support The Supplier will provide an online portal that allows all incidents, service requests and change requests to be log and monitored by users Service desk will be located in the UK at a nominated Supplier location Undertake formal user satisfaction analysis, using a method agreed by both parties Ensure that agreed underpinning agreements are in place with 2nd line support and 3rd parties to	Approx 9500 calls/incidents per annum Approx 2200 change/service requests per annum Hart Approx 1500 calls/incidents per annum Approx 236 change/service requests per annum. This is a total that overall all documents as Hart doesn't split out the different department

<table>
<tr><th>REF</th><th>Service Component</th><th>Requirement</th><th>Frequency / Volumes</th></tr>
<tr><td></td><td></td><td>
ensure that the service can be delivered.

The Supplier shall provide and align the IT service/requirements with ITIL conventions.

All calls to be logged given a priority rating based on the Authorities SLA’s for response.

All change and service requests to be given a priority based on Authorities SLA’s.

Service desk operational office hours:

Monday - Friday 08:00 - 18:00

except bank holidays and national holidays

Incidents
<table>
<tr><th>Level</th><th>Criteria</th><th>Response</th><th>Target</th></tr>
<tr><td>P1</td><td>Whole or critical part of system or network is unusable, causing major business impact</td><td>1 hour</td><td>4 hours</td></tr>
<tr><td>P2</td><td>Important but not immediately critical, part of system or network is unusable. Causes business impact or more than 5 users are affected.</td><td>4 hours</td><td>8 hours</td></tr>
<tr><td>P3</td><td>Inconvenient issue affecting less than 5 users</td><td>8 hours</td><td>20 hours</td></tr>
<tr><td>P4</td><td>Non-urgent issue. Work-around available. Client complaints</td><td>2 Working Days</td><td>5 Working Days</td></tr>
</table>
Response to include assessment of problem and action plan to rectify the issue with quantified estimated time to fix.

Service requests
<table>
<tr><th>Priority</th><th>Criteria</th><th>Completed</th></tr>
<tr><td>P1</td><td>Critical impact or Urgent request for IT services</td><td>1 Working Day</td></tr>
<tr><td>P2</td><td>Standard request for IT services</td><td>5 Working Days</td></tr>
</table>
</td><td></td></tr>
</table>

REF	Service Component	Requirement	Frequency / Volumes

P3	Non urgent request	10 Working Days

Change requests

Priority	Criteria	Assessed	Authorised	Completed
P1	Emergency – To respond to loss of service or severe usability problems to large number of users, or a mission critical system. Major business impact. Immediate action required.	1 Working Day	1 Working Day	5 Working Days
P2	High. Severely affecting some users or impacting upon a large number of users.	5 Working Days	5 Working Days	10 Workings Days
P3	Medium. No severe impact to users or systems.	5 Working Days	5 Working Days	20 Working Days
P4	Low. Cosmetic changes or fixes that do not improve business functional requirements or deliverables	20 Working Days	30 Working Days	40 Working Days

Times and days quoted for each request type start from the logging of the request to the Supplier and are not cumulative.
For example, a P1 change request is to be completed within 5 Working Days of submission. With the assessment and authorisation completed within the first Working Day.

Respond to and evidence customer requests for progress on calls and requests
Updating service desk system with additional information, notes or comments as and when required.

REF	Service Component	Requirement	Frequency / Volumes
		Provide immediate report of P1 incidents to agreed client contacts and analysis report within 2 Working Days of their resolution. Provide scheduled reports for monitoring service desk performance Run ad-hoc management reports as and when requested. Provide client access to service desk system Supplier to provide a minimum of 2 user licences and connectivity to service desk system for each Authority. Provide client access to service desk system for client functions to manage incidents, service and system change requests allocated to the team. Progressing incident calls, service and change requests for customers. Checking status of calls and making sure 2nd line engineers and IT Developers are keeping to SLAs for delivery. Providing timely and relevant communication to user groups on update and status of incidents. Incidents to be closed only, once confirmation from customer that suitable remedial action has been completed. To conduct user satisfaction surveys on completion of incidents, service and change requests.	
IT102	First line support - incidents, service and change requests	Provide a range of first line call support services to complete incidents or service requests at first point of contact. Service desk to deliver first time completion of incidents and service tickets to reduce failure demand to the customer/service teams. Including but not limited to • Password resets • changes to personal details, eg names, phone number, job title etc; on corporate	Approx 800 calls and service requests per annum Hart Approx 292 first time fixes. Other calls passed to 2nd/3rd line

REF	Service Component	Requirement	Frequency / Volumes
		applications, network accounts, email system etc • Email queries - checking and releasing emails in quarantine • virus checking of removable media • releasing locked accounts • answering IT queries • Updates to names or details on telephone system • Create or delete telephone extension information • Issuing loan equipment such laptops – recording information for audit purposes.	
IT103	Systems alert monitoring	Monitor service desk email account for automated alerts. • Check alerts, and log service desk incident or change request as needed to resolve the issue • Action any calls or requests to respond to alerts Patch management • Check patch management system to make sure all systems are being reported and patched • Check why systems are not being patched - raise call with 2nd line support for investigation Log management • Check system log management application for system problems and raise incident tickets for investigation.	
IT104	Mobile phone management	Supplier to provide day to day operation of Authority mobile phone estate. • Raise requests for new connections approved by client • Raise requests and action upgrades to existing connections approved by client • Re-allocate handsets and numbers as needed when officers leave Authority • De-activate connections when numbers closed or handsets lost etc • Check monthly/quarterly invoices and distribute to client cost centre teams • Maintain list of users, sims, handsets (IMEI), cost centres etc, accessible to the	

REF	Service Component	Requirement	Frequency / Volumes
		client	
IT105	Asset Management	Supplier to undertake day to day recording of software and hardware asset management Software: • Recording of software purchases, accessible to client • Checking licence provision to make sure Authorities stay fully licensed • Re-allocating licences of strategic software where need to be redeployed • Removing licences for disposal • Reporting on licence provision • Keep up-to-date list accessible to client of all:- ▪ Software applications in use ▪ Licence numbers and users ▪ Versions ▪ Contract end dates • Notify the Authorities where licences are low or used up to allow for additional purchases • Maintain approved catalogue of software used by the Authorities Hardware: • Recording hardware purchases and asset information into service desk system • Updating service desk when hardware is re-allocated • Updating service desk when assets are removed or retired • Reporting hardware asset disposals • Tag hardware items with Authority asset tag	
IT106	Service Improvement	Identify areas of service improvement, arising out of the user calls/contact and liaise with the Authorities' service management function	
IT107	Out of Hours Support	Out of Hours Support	

REF	Service Component	Requirement	Frequency / Volumes
		Supplier will provide single service desk for both normal working and out-of-hours. Supplier will provide the following services outside Normal Business Working Hours: • Availability Monitoring and Priority 1 registered Incident resolution of Systems • Management of 3rd party escalation where 24 x 7 support services are provided, whereby the Supplier will initiate the 3rd party escalation and monitor progress out of hours. • Configuration changes to supported systems which are required to be undertaken out of hours to avoid disruption to normal daytime Authority operations, subject to a defined limit as described under Change Management. • Patch and minor update of business applications as described under Business Application Support • Onsite services as delivered under the daytime service for out of hours utilisation; • Hardware break/fix maintenance where a 24 x 7 maintenance service is specified and access is available to Authority premises to fulfil the maintenance request • Support of services delivered by the Authorities outside of normal working hours, e.g. point of sale applications, and ticket sales for Cornerstone Arts centre. • Emergency changes to block/close/lock lost equipment that may expose Authority security e.g. laptops, mobile phones etc Out of hours support – Provided by a number of pre payment tokens	

Definitions and Glossary

(to be completed when all Councils have inputted into the requirements. This is intended to provide a glossary for acronyms, Council specific applications or processes etc.)

Term	Definition
Servicedesk / servicedesk	Refers to the function of servicedesk, not any specific software application
ITIL	IT Infrastructure Library. Set of standards for IT service delivery and management
ITSM	IT Service Management
SLA	Service Level Agreement
Failure Demand	demand caused by a failure to do something or do something right for the customer first time
FTF	First Time Fix – incident resolved at first point of contact with Servicedesk

This page is intentionally left blank

Briefing Note

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Meeting Notes

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Scrutiny Project Plan

(Review of the Transfer of IT Services to the Five Councils Contract)

Marketing, Business Development and Five Councils Scrutiny and Policy Development Panel

2016/17

This page is intentionally left blank

SCRUTINY PROJECT PLAN

Scrutiny on the IT Aspects of the Five Councils Contract

SECTION ONE – Project Definition Form

Project Title	*Scrutiny of the IT Aspects of the Five Councils Contract*

Link with the Corporate Strategy and Business Plans	The Council is committed to public service excellence and the IT systems for officers are a fundamental part of delivering all Council services. The Council is also committed to looking at innovative and creative ways to deliver services and the 5 Councils Contract is a leading example of commissioning external companies to deliver a number of services within the Council.
Project Objectives	To understand the implementation plans for the delivery of the IT service within Havant Borough Council
Benefits to the Council and Its Residents	The Council will greatly benefit from a smooth transition to the new IT systems and this will in turn benefit residents.
Evidence to Support the Project	IT has been identified as the major risk of the Five Councils Contract.
Success Criteria:	• To interview key officers to understand implementation plans for IT systems for the Council • To ascertain the concerns of Councillors over the propsed transfer of IT under the contract • To ensure that the concerns raised by Councillors have been or will be addressed • To produce a report to the Scrutiny Board and Cabinet on the implementation of IT systems

SCRUTINY PROJECT PLAN

Scope of the Project	The Project Will Include: A survey of HBC Councillors to ascertain their concerns over the transfer of IT under the 5 Councils' contract Interviews for key internal officers on the implementation plans for IT systems for the Council

Methodology	**Identify the Concerns of the Councillors** Questionnaire **Interviews** Interview Craig Richards, IT Client Manager & IT Work Stream Transition Lead – Five Councils Partnership.

SCRUTINY PROJECT PLAN

Key Officer(s)	Head of Research and Marketing, Head of Programmes, Redesign and Quality

Lead Councillor	Councillor Bains

SECTION TWO – PROJECT PLANNING		
Scrutiny Panel	Marketing, Business Development and Five Councils Scrutiny Panel	
Scrutiny Lead	Councillor Pike	
Panel Members	Councillor G Shimbart, E Shimbart, Blackett, Quantrill, Kerrin	

Witnesses to Interview

Who?	**Why?**	**When?**
Head of Research and Marketing – Dawn Adey	Key officer for 5 Councils Contract	Throughout the review
IT Client Manager & IT Work Stream Transition Lead for the Five Councils Partnership –	Key officer for IT aspect of the 5 Councils Contract	6 December 2016

SCRUTINY PROJECT PLAN

Craig Richards		

Evidence to Gather

(Please identify any information that is key to research for this scrutiny)

Concerns of HBC Councillors on the proposed transfer **Transition plans for IT at Havant Borough Council**

SCRUTINY PROJECT PLAN

Projected Start Date:
6 December 2016

Projected Timescales for:

Evidence gathering – 29 September 2016 – 13 October 2016

Interviews – 6 December 2016

Evidence Analysis – December 2016

Project Report Deadlines

Draft Report Produced – 12 December 2016

Panel to Agree Final Report – 16 December 2016

Dates for:

Report to Scrutiny Board – 31 January 2017 (provisional)

Report to Cabinet – 15 March 2016 (if contains recommendations-provisional date)

This page is intentionally left blank