SOUTHAMPTON
CITY COUNCIL

Internal Audit Report

SCC1819-076

DBO - Mobile Devices

Overall Assurance: No Assurance

CONTENTS

Executive Summary

Introduction, Objectives and Scope

Exceptions Table

Author: Ryan Eayrs
Version: Final
Dated: 29/05/2019
Recipient: Mike Harris (Deputy Chief Executive) John Harrison (Interim Service Director Finance & Commercialisation) James Strachan (Service Director, Business Operations and Digital) Deborah Smart (Service Lead, Digital and Strategic IT) Paul Paskins (Head of Supplier Management) Paul Rickards (Technical Support Officer) Terry Hogan (Technical Support Officer) Lucy Kelly (Sourcing Manager) Tamim Yousefi (Finance Analyst)

Approved by Chief Internal Auditor, Elizabeth Goodwin: P J Somerset

Executive Summary

Employees utilise mobile phones and tablets in their day to day duties in order to communicate effectively and efficiently with internal and external clients and provide an end to end service. The February 2019 bill from the Authority's network provider Vodafone showed there are currently 2,899 devices being charged for. The total contract value was agreed at £369,044, this was based on having 2,733 device plans connected with the network provider.

Compliance with Policies, Laws and Regulations Assurance Level: Reasonable Assurance

The Mobile Phone Usage Policy is available on the staff intranet and states that in order for an employee to be given a mobile device an application must be made through the IS Service Desk and be approved by an appropriate senior manager to confirm it is necessary for the employee's role. The applicant must also declare that they have read and understood the policy.

A random sample of 25 (18%) was selected from a list of 137 requests for mobile phones within 2018 provided by the Technical Support Officer. Testing showed that all requests complied with internal policy and had been authorised by an appropriate senior manager and that all requestors had marked electronically that they had read and understood the internal policy.

A review of the most recent policy found that it was published in May 2016 and was due to be reviewed and updated in May 2018, at the time of testing this had not been completed despite large contractual and procedural changes having taken place. The responsibility for the review, according to the last policy, is split between Human Resources, Finance and IT Services.

A medium risk exception has been raised.

Safeguarding of Assets Assurance Level: Limited Assurance

Testing reviewed what security measures are in place to protect any corporate data accessible via the mobile devices. Audit was unable to look at any live devices, however was able to observe the set up process as demonstrated by the Network Security Analyst. This involves the mandatory installation of an application called SecureApp, which is the encryption program for corporate data. The application requires the user to set up and enter a PIN code (which is separate to the devices standard manufacturer PIN) in order to access any corporate data. Once the correct PIN is entered the device will open any documents within the SecureApp encrypted software, for example if you opened an email it would open in SecureApp's own version of the email application. Users have access to the Google Playstore which means that downloads of Third Party applications are not restricted on employee devices, although corporate data is encrypted on the device. Audit is unable to give full assurance that corporate data is safe from a breach because of malware that could be introduced via Third Party applications.

When each quarterly bill is received from the supplier Finance break the bill down into spend per cost center and a report is made available to senior managers on the network for them to use during budget monitoring discussions. Testing selected 5 users with high usage from the 337 users that had incurred charges above their allowance, on the bill generated in November 2018, the combined charges for the sample selected totaled £3,805.40 (5% of the bill total, £67,275.88). Details of the charges were forwarded to their line managers and Service Lead/ Director to enquire about any action that had been taken and if the managers had been made aware of the charges. All of the recipients responded and advised they were not aware of the charges but would now look to investigate the reason they were incurred. A high risk exception has been raised as a result.

Testing also reviewed how zero usage users are monitored to ensure that employees who were not using their devices had their lines disconnected to avoid further unnecessary charges. The Sourcing Manager in Procurement provided a report generated in August 2018 of users that had not used their devices for the previous 3 months, this process should be completed each quarter. Testing selected 5 (0.5%) of these users from a total of 889 and confirmed whether their device was still active using the most recent bill in February 2019. Testing found that, all 5 had been disconnected accordingly. Another report was ran in May 2019 that revealed 981 devices were shown to have zero usage and were eligible for termination.

A high risk exception has been raised as testing found that no checks are made to confirm the accuracy of invoices before payment. Historically it was the responsibility of Capita to review the quarterly invoices to ensure that the network were charging the authority the appropriate fees in line with the contract, this was previously done by the Technical Support Officer from IT Services but is no longer performed by any party. The Sourcing Manager advised it was the responsibility of IT to check the invoice, as a result testing cannot find any evidence that a formal responsibility exists for someone to check that the network provider is charging the correct amount in relation to the contract.

Following the end of the Authority’s previous contract with Vodafone a new contract was negotiated with the same network provider in 2018, testing selected a sample of employees from a mobile number report generated by Vodafone to ensure that they were being charged in line with the contract terms. A sample of 25 (0.86%) were selected from the 2,899 on the February 2019 bill and 19 of the sample were found to be compliant with the price list set out in the new contract.

The remaining 6 of the sample were being billed at a cost of £43.50 each per quarter to the authority, this information was given to the Sourcing Manager who contacted the network provider and established that the charge was due to a Blackberry Access fee costing £12 a month, and this combined with the £2.50 a month made the total of £43.50. Blackberry Access is an application that allows the user to access the organisation's staff intranets and applications from their mobile device, however the new smartphones have this ability without the additional charge. This is supported by evidence that the Technical Support Officer is working to replace the 398 Blackberry's currently still in use. Testing compared the 6 from the sample with the Technical Support Officers inventory and found that all 6 of the devices were Blackberry's meaning the charge was correct, this also meant that the full sample of 25 were being billed correctly at the time of testing.

Effectiveness & Efficiency of Operations Assurance Level: No Assurance

The mobile phone report from the supplier detailed 2898 devices, testing used information from the internal database in order to reconcile the number of devices in circulation. The Authority's total inventory came to 1,627 devices (mobile phones, tablets and data devices) which represents 56% of the amount the Authority is being charged for quarterly by the network provider, this meant that 1,271 devices were not trackable on IT services' database. Conversations with the Technical Support Officer revealed that before the introduction of smartphones as the standard device back in March 2016 devices issued to employees were not asset tagged and this could account for the reason that many devices could not be found on the internal database.

Using a data analytic software the mobile phone report was matched with a list of all employees from Resource Link. This highlighted 931 devices which could not be matched to a current employee, audit was informed by the Service Lead for Digital & Strategic IT, Business Operations that it is an accepted management practice for mobile devices to be passed between employees when they leave however management should inform IT services when the change of ownership happens. A high risk exception has been raised and further details can be found in the main body of the report.

Completion of the audit Assurance Level: No Assurance

Testing has highlighted three high, and one medium risk exception. As a result Internal Audit can only offer No Assurance that the management of Mobile devices is of low risk to the Authority.

Please be aware that summaries of all exceptions are routinely reported to the Governance Committee who may call in any Audit report they wish. Where any critical exceptions are found and/or the audit receives an overall level of 'No Assurance' these will be reported in their entirety to the Governance Committee along with the Directors comments. These exceptions may also be reported to the relevant Portfolio holder.

ASSURANCE LEVELS

The overall assurance is given on the activity that has been audited.
These levels are based on the areas tested within the audit as noted with the Objectives & Scope.

Levels:	**Description / Examples**
Assurance	No issues or minor improvements noted within the audit but based on the testing conducted, assurance can be placed that the activity is of low risk to the Authority
Reasonable Assurance	Control weaknesses or risks were identified but overall the activities do not pose significant risks to the Authority
Limited Assurance	Control weaknesses or risks were identified which pose a more significant risk to the Authority
No Assurance	Major individual issues identified or collectively a number of issues raised which could significantly impact the overall objectives of the activity that was subject to the Audit

Objectives and Scope

This report outlines the findings from that review and highlights any exceptions considered appropriate.

The objectives of the audit were to ensure that:

Achievement of organisation's strategic objectives

- No areas tested

Compliance with Policies, Laws and Regulations

- Employees that are in possession of work devices have read and understood the council policy on device usage and that this has been recorded. Testing sampled a number of mobile device users to confirm if they had read the relevant policies.

Safeguarding of Assets

- User access is restricted to control third party application downloads, download of documents, access to devices via passcode and other security measures. Testing reviewed how devices are restricted and reported on its effectiveness.
- Appropriate monitoring procedures are in place to review device usage and investigate any abnormal use. Testing reviewed the processes in place and reported on its effectiveness.
- Invoices received are checked for accuracy before payment is made. Testing reviewed the invoice process and tested a sample of invoices to ensure the Authority was being charged in line with its contract.

Effectiveness & Efficiency of Operations

- The inventory of mobile devices is suitably maintained. Testing selected a sample of mobile devices, and evidenced who is currently in possession of the device in order to evaluate the accuracy of the inventory

Reliability & Integrity of Data

- No areas tested

ISS.1 - SCC-1819-076 - Mobile Devices - Mobile Phone Policy	
Priority Level **Medium Risk**	
Exception The Mobile Phone Usage policy was published in July 2016 and contains information on appropriate use of a mobile device and the procedures around obtaining one and returning it to the authority should the device no longer be needed, it also makes reference to the responsibilities of Capita for mobile devices which is a contract in the process of being terminated. It is available to staff via the intranet. Users must confirm they have read and understood before being allocated a mobile device. The responsibility for review of the policy was split between Human Resources, Finance and IT services and it was due to be reviewed in May 2018 the plan to review the policy was on the agenda of the Feb Customer and Digital Board.	
Risks and Consequences Failure to ensure that internal policy is kept up to date could result in procedure not being followed by employees, if processes have changed then employees would be unaware aware of it without an up to date policy to reflect the changes. Any contractual changes that have occurred would also not be evident in the internal policy and may cause mismanagement of assets belonging to the Authority.	
Agreed Action	**Person Responsible / Action by Date**
Continue with the planned review of the mobile phone policy.	Deborah Smart – June 2019

ISS.2 - SCC-1819-076 - Mobile Devices - Inventory

Priority Level
High Risk

Exception

A reconciliation between the mobile phone report from Vodafone (2898 devices) and the mobile device inventory on the internal database noted that 1271 devices were not noted within the inventory.

Further testing was conducted to compare the mobile phone list with a list of all employees from Resource Link in order to identify devices which are registered to individuals who are no longer employed by the Authority. This match highlighted 931 devices which could not be matched to an existing employee. The total expenditure across all 931 devices for the last quarter (Nov 18 - Jan 19) was £10,843.91

It was noted during testing that 80 devices were registered to a generic team or Authority name which further complicates identifying who is in possession of the device.

The list of 931 devices was matched with the latest usage report from Vodafone for the period November 2018 - January 2019 which showed that:

- 272 mobile phones that had no usage at all (no calls, no text messages or data use) costing £3234.25 in plan charges for the last quarter
- 124 Data Only devices (which are not capable of calls or text messages) used no data for the period costing £744 in plan charges for the last quarter
- 535 devices are being used in some capacity be it calls, text messages or data which cost £6865.66 in plan charges

Risks and Consequences

Failure to keep proper tracking of inventory could lead to financial losses within the Authority and failure to distribute resources effectively. Devices could be stolen without the Authority knowing who was last in possession of the phone or tablet. When an employee leaves the Authority if there is no record of them having a phone it is unlikely to be stopped and the Authority will continue to be charged resulting in a financial loss.

Agreed Action	Person Responsible / Action by Date
Present at Executive Management Board audit findings and seek agreement to endorse following action • Managers to provide list of devices against named personnel • Agreement that as staff leave the devices will be returned to IT for reallocation etc • Any SIMS or data where a named individual cannot be identified will be disconnected. Ownership from all Service Directors Managers to provide IT with up to date information about who has mobile phones and tablets and return any that are not required to IT for destruction and contract termination.	Service Leads - June 2019

ISS.3 - SCC-1819-076 - Mobile Devices - Monitoring

Priority Level
High Risk

Exception
Testing reviewed what procedures were in place to detect high and zero usage users in the quarterly bills generated, this was to ensure that the authority could investigate any issues with employee usage. The Finance Analyst advised that when the quarterly bill is received it is broken down into cost centres and it is stored on a network drive so it is available to the department and their corresponding finance analyst and can be discussed in their monthly budget meetings.

As a result of this 5 examples of high usage (above the allowance) were selected from the November 2018 bill as at the time of testing the February charges had not been distributed. An email was sent to each employee's manager and Service Lead/ Director to enquire if they were aware of the charges incurred in that particular bill and if they were what steps had been taken to investigate the issues.

A report was generated in August 2018 that detailed 889 devices that were listed as zero usage and were eligible for termination. Another report was generated in May 2019 that provided information for 981 devices that were listed as zero usage and were eligible for termination.

No evidence of monitoring was found as a result of testing, of the 5 line managers/ Service Leads/ Directors that were emailed none of them were aware of the charges incurred by their employees on their mobile devices and when it was highlighted they requested further information so that they could investigate it. An amount of £3,805.46 in November and £431.98 in February's bill were due to usage charges from employees, the process detailed by the Finance Analyst whereby cost centre's would review mobile devices as part of their spends on a quarterly basis was not found to be adequate.

Risks and Consequences
Failure to properly monitor employee usage can lead to additional charges to the Authority as evidenced in testing.

Agreed Action	Person Responsible / Action by Date
Exceptions reports with high and unusual usage (i.e. international calls etc) will be produced and analysed and provided to the budget holder for that relevant areas for investigation and action.	Sourcing Manager - Procurement (Lucy Kelly)

Sourcing Manager - Procurement to make the invoice authorising officer aware of any major issues that may impact on their decision to authorise payment. Finance business partners to go through mobile bills with budget holders on a quarterly basis	Sourcing Manager - Procurement (Lucy Kelly) Finance Business partners - quarterly with effect from May 2019

ISS.4 - SCC-1819-076 - Mobile Devices - Invoices

Priority Level
High Risk

Exception

Testing selected a sample of 25 (0.86%) from 2,898 lines present on the bill in February 2019 with a mixture of different mobile lines, this included Voice only, Voice and data and Data only lines. 6 of the samples charges could not be identified in the contract, each of these 6 devices was costing the Authority £43.50 per quarter, the remaining 19 of the sample tested were being charged in accordance with the current contract. Audit provided details of the 6 discrepancies to the Sourcing Manager who subsequently contacted the network provider who advised that the charge is for Blackberry device users and a fee of £12.00 per month for Blackberry Access, which is a software that allows users to access the organisation's intranet pages and applications from their mobile devices, this £12.00 per month coupled with the standard line cost of £2.50 totaled £43.50 for the quarter. This is a charge that will remain until the 398 Blackberry's in circulation are replaced with smartphones, this is something the Technical Support Officer is currently progressing and keeping a record of, audit also compared the users against the inventory to ensure they had Blackberry devices and it was found that they did so the charge was appropriate.

As a result the sample of 25 tested did indicate that the February 2019 invoice was issued in line with the contract and contained the correct charges.

Discussions with different officers from IT and Procurement who are employed by Capita and subsequently officers from Finance, and HR who are employed directly by the Authority identified that historically the responsibility of checking the quarterly invoices received from the network provider was that of a Technical Support Officer from the Capita IT services however since the contractual changes with Capita this was not in place at the time of testing. It was identified that there is no formal or informal responsibility present amongst the departments questioned for verifying that the charges from the network provider remain in line with the contract each quarter.

Risks and Consequences

Without checks to quarterly invoices the authority cannot give assurance that the network provider is billing them correctly in line with the contract in place and could open the authority up to a financial risk. Failure to ascertain what the Authority should be paying on a quarterly basis could lead to a discrepancy in budget and forecasting for the Authority's resources.

Agreed Action	Person Responsible / Action by Date
In line with the mobile phone policy review make sure the roles and responsibilities for managing the devices and contracts are clear and communicated to all. This needs to include bill checking Also actions above	Deborah Smart – June 2019

EXCEPTIONS

The following tables outline the exceptions from the recent audit and are reported in priority order. Internal Audit report regularly to the Governance Committee on findings and management actions. However, in accordance with agreed protocols, all critical exceptions are brought to the attention of the Committee.

Priority Level	Description
Critical Risk	Control weakness that could have a significant impact upon not only the system function or process objectives but also the achievement of the organisation's objectives in relation to: ▪ The efficient and effective use of resources ▪ The safeguarding of assets ▪ The preparation of reliable financial and operational information ▪ Compliance with laws and regulations And corrective action needs to be taken immediately.
High Risk	Action needs to be taken to address significant control weaknesses but over a reasonable timeframe rather than immediately. These issues are not "show stopping" but are still important to ensure that controls can be relied upon for the effective performance of the service or function. If not addressed, they can, over time, become critical. An example of an important exception would be the introduction of controls to detect and prevent fraud.
Medium Risk	These are control weaknesses that may expose the system function or process to a key risk but the likelihood of the risk occurring is low.
Low Risk - Improvement	Very low risk exceptions or recommendations that are classed as improvements that are intended to help the service fine tune its control framework or improve service effectiveness and efficiency. An example of an improvement recommendation would be making changes to a filing system to improve the quality of the management trail.