Appendix B - Payables

Executive Summary

A fundamental system audit of Payables has been carried out as part of the 2017/18 Audit Plan. The authority's financial procedures rules set out the responsibilities of employees tasked with paying creditors to ensure the authority is paying creditors in a timely, correct manner while minimising the risk of fraud and also comply with the Late Payments of Commercial Debts (Interest) Act 1998. This audit has looked at the Agresso accounts payable system and the feeder system Total.

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

Local Government Transparency Code 2015

One high risk exception has been raised and is currently under investigation, the details of the exception can be found under ISS 7.

The Local Government Transparency Code 2015 makes it mandatory for the authority to publish details of all expenditure that exceeds £500, at least on a quarterly basis. The authority is publishing financial spend over £500 in the correct format and frequency to ensure compliance with the Local Government Transparency Code 2015. To ensure reports are correctly formatted and do not contain any private and sensitive information the dataset must go through a process of anonymisation where some payments to individuals will have the supplier name redacted. In the October to December 2017 report published anonymisation had not taken place causing payments made to individuals being accessible to any member of the public. The report in question also included detailed reasoning for the individual payments due to the file uploaded being the internal file used by service areas to check all payments are accounted for before publication. This file contained sensitive personal information relating to payments, for example legal fees and foster care payments breaching the Data Protection Act 1998.

Safeguarding of Assets Assurance Level: Limited Assurance

Total – Housing Operations System

One high risk exception has been raised, under ISS 1, with a number of the agreed actions already implemented and action taken immediately to administer access.

Although Total access has roles assigned to users these roles do not reflect the level of access members of staff have to the Total system. When staff have had access setup it has not been customised for the role they are undertaking which has led to members of staff having a level of access far greater than what is required to complete their jobs. Users have the ability to close or cancel jobs, amend or cancel invoices and change the quantity of materials used. Although some of these roles would be required for some users to undertake their job effectively, there is currently a lack of consideration as to which roles require which level of access and has resulted in an 'all or nothing' approach to Total system access. This risk of a lack of refined system access is exaggerated with the lack of management oversight into invoices cancelled, the amount of issued credit notes and the amount of invoices being paid without a purchase order.

Agresso Privileges

One low risk exception has been raised as detailed under ISS. 5, an agreed action has been completed to mitigate risk.

To ensure that access to Accounts Payable privileges are adequately controlled an Agresso access report was requested on users who have full access to the supplier Masterfile. Testing found that from a list of 28 users with the MACREDITORS role, 3 (10.71%) no longer needed access due to them leaving the authority. At the time of testing this information was provided to the Service Manager who requested that leavers had their access removed. Further testing was undertaken on the SUPER role used by the Agresso helpdesk which found that 1 out of 8 users no longer needed access due to them leaving the authority.

Effectiveness & Efficiency of Operations Assurance Level: Limited Assurance

Manager Authorisations

One high risk exception has been raised under ISS 3. In order to address this issue fully, buy in by services across the authority will need to be obtained to reduce the amount of outstanding authorisations.

Before a payment can be made it requires the authorisation of a manager, testing was conducted to ensure that managers were reviewing invoices in a timely manner. A review of data extracted from the supplier portal found there were 1,420 invoice payments awaiting authorisation which had been received at least 30 days earlier. Which is a breach of the Late Payments of Commercial Debts (Interest) Act 1998 for undisputed invoices and the

authority could be forced to pay statutory interest on the total gross amount (£858,635.59). These payments were spread over 112 different suppliers with *Company A* accounting for 1,138 (80.14%) of the 1,420 late payments. There were 71 different approvers who were responsible for authorising these late payments with a further 33 payments having a blank authoriser. These late payments were further broken down into the system they originated from, out of the 1,420 late payments, 1,246 (87.75%) originated on Total, 167 (11.76%) on Agresso and 7 (0.49%) on Paris.

Goods Received Notes & Auto Matched Payments

One high risk exception has been raised under ISS 2. This finding has already identified as a priority during implementation of the new 'Enterprise Resource Planning' upgrade to 'Business World' with action going to be taken immediately to no longer provide the option to bypass goods received notes. This will require buy in by services to ensure this doesn't significantly increase the amount of late payments.

A goods received note (GRN) is an internal document which is designed to record and confirm that the items received match the purchase order before payment is made. At present the payment run bypasses goods received notes meaning that orders are put into the payment run without the validation that they have been received in the correct quantity and are not faulty or damaged. Instead if the Bypass MGRN box is ticked then the invoice goes to the authoriser again before the payment is made.

Automated payments reduce the amount of manual intervention required due to the accounts payable team not having to go through the purchase order, goods received note and invoice for individual orders, instead only having to deal with payments where there is a discrepancy between these documents. Out of the 62,458 payments made this financial year up to the point of testing, only 5,337 (8.55%) auto matched due to a goods received note being completed and matching the purchase order and invoice. A further 129 payments would have auto matched but were over the £10,000 limit so the workflow sent them to be authorised. Furthermore, at the time of testing no tolerances levels were setup in Agresso to auto match minor discrepancies.

Duplicate Payments

One high risk exception has been raised under ISS 4. Moving forward audit will conduct regular data analytics testing to aid the service in the identification of potential duplicate payments.

A spread sheet of payments was extracted from the supplier portal and data analysis software was used to detect any duplicate payments to test the mechanisms in place to avoid and detect duplicate entries. The data analysis software produced four reports which listed 88 payments which had the possibility of being duplicates. From this list testing was conducted on 25 and found 15 of the 25 payments were potentially duplicate payments due to

them having no discernible differences in detail. The value of the payment and corresponding duplicate totalled £175,241.39, meaning that the authority paid at least £87,620.70 in repeat payments. For three of these duplicate payments recovery action had already been undertaken after they had been identified by the Accounts Payable team or individual service areas. If this sample was consistent over all 88 of the possible duplicate payments then there is potential for 53 duplicate payments to have occurred over the seven month period.

Sensitive Data on Invoices

One high risk exception has been raised under ISS 8. Work will be undertaken immediately between nominees from Legal, Children's Services and Finance to consider new arrangements that work within available resources.

During the suspected duplicate testing three (12%) invoices were identified that had the name and date of birth of a child written on them. The invoices were found to be for services of a sensitive personal nature. Further testing was conducted by searching the SC200 cost centre and found personal data being recorded since at least 2008 where an individual's name was recorded next to a payment for a psychiatric test. Testing also found payments for several other types of fees include paternity tests which the three children of the parent in question had their names and date of births recorded, a cognitive assessment and family court fees. The Agresso helpdesk provided an access report which concluded 538 users were able to view invoices and financial information under the cost code these payments were coded to.

Staff Training and Procedure Notes

No issues have been raised with the training and documentation provided to the Account Payable & Client Monies team.

To ensure new starters within Accounts Payable are provided with adequate training they will be assigned a buddy who will demonstrate to them how to complete certain processes and as they grow into the role they will be given greater responsibilities. Once management is happy that they have had the necessary training and have demonstrated the right skills for a specified task this will be recorded on the Skills Matrix. The Skills Matrix is comprehensive and lists responsibilities for scanning, creditors, technicians, adults and CMS into 90 separate tasks. Furthermore, staff performance in undertaking invoice processing on Db Capture and Total is monitored against errors found during the daily audit undertaken by supervisors.

As part of the review, Internal Audit observed the payment run procedures to ensure that they accurately reflect the processes and procedures in place. From this walk through and an analysis of the procedure documentation, Internal Audit can conclude that the payment run documentation is comprehensive enough to ensure that there can be no operational ambiguity in regards to the payment run process. There was also an analysis

undertaken on the maintenance of the supplier Masterfile procedure documentation which is comprehensive but the documentation needs some minor revision to accurately reflect the current procedures in place. This position was originally highlighted in the initial audit meeting and work is underway to update this documentation.

Reliability & Integrity of Data Assurance Level: Reasonable Assurance

Duplicate Suppliers

One medium risk exception has been raised under ISS 6. Moving forward audit will conduct regular data analytics testing to aid the service in the identification of potential duplicate suppliers in the Masterfile.

The processes and controls in place in the accounts payable team ensure that new suppliers records added to the supplier Masterfile are sufficiently validated against invoices before getting authorised. Any request to amend a supplier record must be in writing whilst requests requiring a change to bank details must be validated by contacting the company using contact details currently on file. Any change of bank details also requires a change of bank details form to be completed and signed off by the person who filled in the form, the person who updated Agresso and the person who checked the amendments. When the necessary changes have been completed the paperwork needs to be passed over to another member of the team to be checked and completed. Testing was conducted to ensure that the supplier Masterfile was free from duplication using data analysis software. It was found that 32 (0.41%) out of the 7850 suppliers had at least one duplicate supplier entry on the supplier Masterfile.

Completion of the audit Assurance Level: No Assurance

Six high, one medium and one low risk exception have been raised as a result of this audit. Based on the testing conducted Internal Audit can offer no assurance that the payment processes currently in place are of low risk to the authority or that they are safeguarding the authority's funds. Although the payment runs taking place are set up to run effectively and payments are being made, adherence to the defined process is not taking place across the authority resulting in a significant number of incidents which are having a detrimental impact on the control framework in this area.

Appendix B

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