|  |  |
| --- | --- |
| C:\Users\vanessa.blackburne\Desktop\Rooster\tiaa.jpg |  |

|  |
| --- |
| **The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police** |
| **Assurance Review of Key Financial Controls** |
| **2017/18** |

|  |
| --- |
| **Executive Summary** |

|  |  |
| --- | --- |
| **OVERALL ASSURANCE ASSESSMENT** | **OVERALL CONCLUSION** |
|  | |  |  | | --- | --- | | **There are appropriate controls in place and operating for the majority of the processes reviewed;** | | |  | **Supplier details changes could be strengthened to mitigate against potential fraud.** | |  | **Robust processes are operating for Accounts Payable and Accounts Receivable which include clear segregation of duties.** | |  | **Treasury management arrangements are appropriately directed and well controlled.** | |
| **SCOPE** | **ACTION POINTS** |
| The review assessed the adequacy and effectiveness of the internal controls in place at the Constabulary for managing the following key financial systems: Accounts Receivable; Accounts Payable; General Ledger and Treasury Management.  The review considered that financial transactions were complete and accurately recorded on a timely basis within the Financial Ledger, thus ensuring the integrity of all financial information reported, included management accounts and financial accounts. | |  |  |  |  | | --- | --- | --- | --- | | **Urgent** | **Important** | **Routine** | **Operational** | | **0** | **2** | **1** | **0** | |

|  |
| --- |
| **Management Action Plan - Priority 1, 2 and 3 Recommendations** |

| **Rec.** | **Risk Area** | **Finding** | **Recommendation** | **Priority** | **Management**  **Comments** | **Implementation**  **Timetable**  **(dd/mm/yy)** | **Responsible**  **Officer**  **(Job Title)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Compliance | It was advised that the Oracle system does not permit a report to be run to identify when supplier banks details have been changed.  Testing identified that the checking of supplier details changes is not undertaken as a standard control, although there was evidence to support that it had been undertaken for four out of five bank account changes that were able to be identified from hardcopy paperwork held by the Finance team. | All supplier account details changes be verified with the supplier using existing contact details before the change is made. | 2 | *Note: there is an audit log which identified who made the last change to an account. However we have since written a bespoke report which provides greater clarity regarding the changes.* | *31/12/17* | *Ged Gallagher* |
| 2 | Compliance | It was advised that the Oracle system does not permit a report to be run to identify when supplier banks details have been changed.  The use of having such a report would allow a check of any changes that may have been made between each payment run. | Investigations be undertaken to identify if the Oracle system can be utilised to provide a report that identifies supplier detail changes, which would allow a check to be undertaken prior to each payment run. | 2 | *Note: there is an audit log which identified who made the last change to an account. However we have since written a bespoke report which provides greater clarity regarding the changes.* | *31/12/17* | *Ged Gallagher* |
| 2 | Compliance | A review of the user accounts on Oracle for Accounts Payable and Accounts Receivable noted that there were four users plus an Administrator who had Receivables Super User Status, however, it was identified that three of these also had a separate account designated as Receivables User, which appeared to be a duplicate. | A review of the duplicated accounts with Receivables Super User and Receivable User permissions be undertaken to determine if both accounts are required. | 3 | *Note: These were not duplicate accounts. The user only had one account to access the system, however the account had two levels of responsibility within the account. We have removed the lower level as it was established the functionality within the “Super User” was the required level for the role.* | *30/11/17* | *Ian Hailstone* |

|  |
| --- |
| **Operational Effectiveness Matters** |

| **Ref** | **Risk Area** | **Item** | **Management**  **Comments** |
| --- | --- | --- | --- |
| There were no operational effectiveness matters identified. | | | |

|  |
| --- |
| **Detailed Findings** |

**INTRODUCTION**

1. This review was carried out in October 2017 as part of the planned internal audit work for 2017/18. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

**BACKGROUND**

1. The Force utilises an external provider, Sopra Steria, for the back office financial arrangements. In relation to this review, this includes accounts payable and the accounts receivable function, as well as the general ledger journals. The treasury management aspect of this review is undertaken by the Treasury team, who are OPCC staff.

**MATERIALITY**

1. For the first six months of the 2017/18 financial year 303 invoices have been raised to a net total of £2.25M. In the same period, 5,859 invoices have been paid, totalling £6.07M.

**KEY FINDINGS & ACTION POINTS**

1. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

**SCOPE AND LIMITATIONS OF THE REVIEW**

1. The review assessed the adequacy and effectiveness of the internal controls in place at the Constabulary for managing the following key financial systems: Accounts Receivable; Accounts Payable; General Ledger and Treasury Management. The review considered that financial transactions were complete and accurately recorded on a timely basis within the Financial Ledger, thus ensuring the integrity of all financial information reported, included management accounts and financial accounts.
2. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

**DISCLAIMER**

1. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

**RISK AREA ASSURANCE ASSESSMENTS**

1. The definitions of the assurance assessments are:

|  |  |
| --- | --- |
| **Substantial Assurance** | There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved. |
| **Reasonable Assurance** | The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved. |
| **Limited Assurance** | The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved. |
| **No Assurance** | There is a fundamental breakdown or absence of core internal controls requiring immediate action. |

**ACKNOWLEDGEMENT**

1. We would like to thank staff for their co-operation and assistance during the course of our work.

**RELEASE OF REPORT**

1. The table below sets out the history of this report.

|  |  |  |
| --- | --- | --- |
| **Date draft report issued:** | 17th October 2017 |  |
| **Date management responses received:** | 1st November 2017 |  |
| **Date final report issued:** | 6th November 2017 |  |

1. The following matters were identified in reviewing the Key Risk Control Objective:

|  |
| --- |
| **Directed Risk: Failure to direct the process through approved policy & procedures.** |

* 1. The Joint Corporate Governance Framework, that was last reviewed and updated in 2016, includes the Financial Regulations and Standing Orders for the Force. Adequate direction for the operation of accounts payable, accounts receivable and treasury management is included, along with any relevant delegated limits. The Financial Regulations make explicit reference to the requirement to have segregation of duties.
  2. In addition to the Financial Regulations there is a documented Annual Investment Strategy; the most recent review was undertaken in February 2017 for the 2017/18 version. It was noted that the Prudential Indicators for Treasury Management were also reviewed at this time, which affords compliance with the CIPFA Prudential Code of Practice.
  3. Procedures are documented for the Accounts Payable, Accounts Receivable and cover the following processes within the areas covered by this scope:
* Raising Invoices;
* Setting up a Supplier;
* Changing Bank Details on a Supplier;
* BACS Payment Run;
* Cheque Payment Run;
* Setting Up a Customer; and
* Producing Debt Reminder Letters.
  1. In relation to Treasury Management there are documented procedures for Cash Flow Management, Investments and BACS processing.
  2. Procedures are also documented for the management of the Chart of Accounts and the raising and processing of journals.

|  |
| --- |
| **Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.** |

**Accounts Payable**

* 1. Twenty invoices raised by the Force in the first six months of 2017/18 were selected for review. For each invoice in the sample there was a fully completed and authorised pro-forma along with the relevant budget code. It was also noted that each pro-forma had been checked and validated by the Finance Team before processing.
  2. Invoices are then system matched to Purchase Orders and Good Receipted, which allows the invoice to proceed for payment when due. Any invoices where the match cannot be made are placed on 'hold'. A weekly ‘Hold Report’ is provided to the relevant requisitioners so that they can review and progress any invoices that are unable to be matched. An overnight validation is automatically run to pull these invoices through to payment stage following review.
  3. Invoices where there is no purchase order quoted are generally returned to the supplier for further information and resubmission. The exception would be where the invoice relates to a key service or supplier, for which contact with the supplier would be made to clarify the details.
  4. It was noted that all Fleet related invoices are passed to the Fleet management team for individual review and coding.
  5. A sample of 15 invoices paid during the three months from June 2017 was reviewed. The sample contained 11 invoices that were system matched and four that were subject to manual review. In each case the invoice was evidenced and had been matched to the correct purchase order, or had been subject to review and been duly authorised. Where the invoice had been manually authorised the audit trail was evident and the payments had been authorised in accordance with delegated levels of authority.
  6. A signature list for approvers is held by the Finance Team and was last updated in September 2017
  7. A sample of 10 new suppliers that were set up in the three months from June 2017 was reviewed. This equated to circa 10% of the new accounts in the period selected. For each supplier a Supplier Setup Form was evidenced that had been completed by the originator and subsequently authorised. It was noted that on receipt of the form the Finance Team review the information and carry out additional checks to confirm that the payments details do not already exist on Oracle.
  8. It was advised that the Oracle system does not permit a report to be run to identify when supplier banks details have been changed. As such a sample of five changes made in July 2017 was selected through a manual review of documentation held on file. For four of the changes reviewed there was evidence to support that a verification was undertaken using existing contact details. It was however, noted in discussions, that this is not a practice adopted for all change requests. This was borne out by the remaining change in the sample, where emails with an attachment had been received by the Force providing the new details, with no subsequent check evident. This should be undertaken for all changes requested, not just those relating to supplier bank account details.
  9. One approach used by fraudsters is to request that contact details are changed on the system (prior to submitting a bank account change request) as these tend not to be subject to the same level of scrutiny by employees.
  10. Another approach is for fraudsters to contact an organisation’s suppliers (pertaining to be the targeted organisation) requesting that they submit copies of all outstanding invoices. If obtained, this gives the fraudster knowledge of the organisation’s point of contact for account payments, contact details (normally email) and outstanding invoices, which can then be doctored to include a new bank account details section. Again, such change requests tend not to be subject to the same level of scrutiny by employees.
  11. Fraudsters are clearly becoming more ingenious in their approach requesting such changes and it is important that the organisation has processes in place to mitigate against the risk of this occurring. It should therefore be ensured that the same verification process is utilised in order to verify the authenticity of all changes made.

|  |  |
| --- | --- |
| **Recommendation: 1** | **Priority: 2** |
| **All supplier account details changes be verified with the supplier using existing contact details before the change is made.** | |

|  |  |
| --- | --- |
| **Recommendation: 2** | **Priority: 2** |
| **Investigations be undertaken to identify if the Oracle system ca be utilised to provide a report that identifies supplier detail changes, which would allow a check to be undertaken prior to each payment run.** | |

**Accounts Receivable**

* 1. Twenty invoices raised by the Force in the first six months of 2017/18 were selected for review. For each invoice in the sample there was a fully completed and authorised pro-forma along with the relevant budget code. It was also noted that each pro-forma had been checked and validated by the Finance Team before processing.
  2. An aged debtors report was generated during the audit visit which showed that the total amount due was £1.237M, of which £1.144M was recorded as 61+ days overdue. Further analysis identified that there were a number of disputed invoices that amounted to £1.078M, leaving an amount of just under £70k overdue.
  3. A sample of five accounts was selected for review. For each account there was evidence to support the outstanding balance and the actions taken to recover. These included two accounts where an agreement was in place to recover the monies over a period of time. Evidence was provided to support the debt reminder letters being sent to overdue accounts as well as diary notes to support email and telephone contact.

**Treasury Management**

* 1. At the time of the audit assignment visit there were six investments made across four counterparties. Each investment was confirmed to have been made in accordance with the policy.
  2. An annual cash flow forecast is prepared in advance of the start of each financial year. Expected income and expenditure is collated from across the Force, with the 12 month forecast being prepared by the two Treasury Managers, which is subject to review by the Deputy Finance Manager and the CFO. A checklist has been developed that covers the key areas, to assist in the completeness of the forecast. A comprehensive audit trail of the information used to prepare the 2017-18 forecast was evidenced during the audit visit.
  3. The forecast is held on Excel and is password protected. As each month progresses the forecast is updated with actual figures and a month end review identifies any difference, which is then investigated to assist with the following years forecasting process.
  4. A daily cash flow is also maintained, which is reconciled to the bank statements that are downloaded each morning.
  5. Month end routines include a reconciliation of bank accounts. A review or reconciliations undertaken in July and August 2017 was undertaken. The four reconciliations required each month were completed by 10am on the first working day of the following month for the sample reviewed and were signed as being prepared by the Treasury Manager and checked by the Deputy Finance Manager.
  6. Month end ledger reconciliations were reviewed for July 2017. A full audit trail of hardcopy documents signed by the preparer (Treasury Assistant) and the reviewer (Treasury Manager) were evidenced. A checksheet is used to show sign off by the Deputy Finance Manager, which was dated the 21st of the following month.
  7. Procedures for the BACS payment run process has been documented and is supported by system screen shots. Weekly payment runs are processed every Thursday with the Treasury Team being provided with an email from the Finance Team at Sopra Steria confirming that the payment run has been scheduled, its reference number and the total value of the payments.
  8. The Treasury Manager reviews the Cashflow and confirms to the Finance Team that the payment run can proceed. A review of expected payments is also undertaken at this time.
  9. A BACS payment schedule is then created by the Finance Team, which is then picked up by the Treasury Team through the Albany system. BACS payments are then released by one of the authorised card holders utilising the card reader and individual passwords. There are five authorised cardholders who can release payments.
  10. A BACSTEL-IP Submissions Summary report is generated on completion of the authorisation process which confirms that the payments have been accepted by the bank for onward transmission. The report records each individual payment as well as any rejected items, which are then subject to further review with the Finance Team.
  11. A sample of five BACS payments made during the three months from June 2017 was reviewed. Summary reports along with an audit trail to confirm the interaction between the Finance and Treasury Teams were evidenced for each BACS payment run. There were no rejected items in the sample selected.

**General Ledger**

* 1. A Chart of Accounts is maintained with any changes requiring a duly completed Oracle Coding Request pro-form\ (A 02-10) being completed, which is subject to review and approval by the Lead Finance Business Partner. Amendments to Components can only be made by the Senior Management Accountant and the systems and Account Manager. Combinations within components changes can be made by staff within the management accounting team.
  2. A procedure is documented for the change process.
  3. A sample of five new account code requests was reviewed. For each code a duly completed and authorised Oracle Coding Request was evidenced that accorded with the code on Oracle.

**Oracle System**

* 1. Access to Oracle for users is controlled through specific user permissions based on the allocated role. Accounts can only be set up on receipt of an auto generated email which follows an account being authorised by HR. A basic account that allows access to the CP Employee Self Service system is initially set up, with any additional permissions for users only being applied on receipt of an authorisation from the relevant Business User Manager.
  2. A review of the user accounts on Oracle for Accounts Payable and Accounts Receivable was undertaken. The following was noted:
* For Accounts Payable, there were multiple users who had read only access, which included staff working on the Service Desk.
* Three users had Accounts Payable access, which accorded with the staff involved in the process; and
* There were four users plus an Administrator who had Receivables Super User Status, however, it was identified that three of these also had a separate account designated as Receivables User, which appeared to be a duplicate.

|  |  |
| --- | --- |
| **Recommendation: 2** | **Priority: 3** |
| **A review of the duplicated accounts with Receivables Super User and Receivable User permissions be undertaken to determine if both accounts are required.** | |

---------------