THE POLICE AND CRIME COMMISSIONER FOR CLEVELAND AND THE CHIEF CONSTABLE OF CLEVELAND

Key Financial Controls

Internal audit report 2.21/22

FINAL

22 October 2021

1. EXECUTIVE SUMMARY

Why we completed this audit

A review of key financial controls process has been completed to provide assurance that the Force's financial system is appropriately managed to ensure that all financial transactions are adequately recorded. Our review also considered the controls that are in place for both accounts payable and accounts receivable and that these are appropriate and are working as intended.

The Force has a Corporate Governance Framework which includes financial regulations that are used to govern the Force's use of funds and outlines the responsibilities for key individuals such as the Chief Constable, the Commissioner and the Force's Chief Financial Officer. The Force uses the Oracle finance system to manage its financial processes which includes the general ledger and purchase order requisition and approval. An authorised signatories list has also been created and regularly monitored and updated to include all individuals who can approved purchase orders. This has been built into the Force's finance system to ensure additional controls are in place. A month-end procedure document has been implemented to outline the process that staff must use at month-end and includes a step-by-step guide for each stage. Bank reconciliations are completed by the Treasury Team and are reviewed and approved by the Strategic Finance Manager.

As part of the audit, we have conducted IDEA data analytics to conduct more in-depth and accurate testing of Force financial data. This has included testing to determine duplicate payments, duplicate suppliers and bank details and purchase order approval by individuals that are not included on the authorised signatory list. We have conducted sample testing following completion of the IDEA testing to identify any discrepancies. Management have been provided with copies of the IDEA results to review and action if necessary. Results of the IDEA testing and sample testing can be seen in Appendix B.

Conclusion

As a result of our review, we have agreed **one low** priority management action. In addition, we have raised **one suggestion** for management consideration.

Our review saw the completion of IDEA data analytics testing with a summary of the results in Appendix B. Following this testing we conducted sample testing to determine any discrepancies however no issues were identified (other than a problem with the report printed from the Oracle system). Management should consider and review the results of the IDEA testing to determine if there are any areas of concern.

We have also included one suggestion for management consideration which is to ensure that the procedure document date of review is updated when reviewed at the end of the month.

Internal audit opinion:

Taking account of the issues identified, the Police and Crime Commissioner for Cleveland and the Chief Constable of Cleveland can take **substantial assurance** that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied and effective.

Key findings

Following our audit testing, we have raised one low priority management action:

We have completed IDEA data analysis testing on a number of areas and the results have been provided to the Force for further review. We have also selected samples from these results and tested these with management. A full summary can be found on Appendix B. There is a risk that if these results aren't reviewed, anomalies and discrepancies identified during the testing may go unnoticed. **(Low)**

In addition, we have raised a suggestion which detailed in section two of this report.

Our audit review also identified that the following controls are suitably designed, consistently applied, and are operating effectively:

The Force has a set of financial regulations within the Corporate Governance Framework which govern the use of Force funds and set out individual responsibilities. An authorised signatory list is also available alongside the financial regulations to help ensure the Force is aware of which staff member can approve purchase orders and their authorisation limit. This has been translated onto the Oracle system to ensure authorisation limits cannot be exceeded.

A month-end procedure document is in place which provides a step-by-step guide for staff when completing the month-end process. Each step is supported by screenshots from Oracle and includes key responsibilities at each step (for example the Lead Finance Business Partner should review Finance reports before inputting these onto Oracle).

Control account reconciliation is completed on a monthly basis and we have confirmed this process is completed through review of the three most recent months (July, August and September 2021). For all three months we have been provided with the documentation showing the control account reconciliation review and approval and have confirmed through email trails that this has been signed off by the appropriate individual.

A new supplier form is required for all new suppliers and is used to input details onto Oracle (such as bank details and supplier address). We selected a sample of 20 new suppliers and confirmed that the new supplier form matched the Oracle finance system for 19 of the 20 suppliers. For the remaining supplier, we noted that the bank details on Oracle were different to those on the new supplier form. Upon review and discussion with

management we confirmed that an email trail had been saved on file confirming that the supplier's details had changed to the details on Oracle. We confirmed that this email trail was after the new supplier form had been completed which explained the initial discrepancy.

Purchase order requisitions are required to be approved by authorised individuals and the value of each purchase order should not exceed the approver's limit. We selected a sample of 20 purchase orders (POs) and confirmed that the purchase order had been approved by an authorised individual (as per the authorised signatories list), the value of the PO did not exceed their limit and the PO had been raised and approved before the invoice had been received. For 16 of the 20 purchase orders, we confirmed that they had been approved by an authorised individual, before the invoice had been received and did not exceed the approver's limit. One PO has been appropriately authorised however an invoice has not been received. For the remaining three POs we noted that they had been authorised correctly however they had been raised retrospectively after an invoice had been received. We queried why this occurred and were informed that one instance was an emergency in which equipment had to be purchased and that the other two instances were due to agreements and contracts that had been made and signed off by the appropriate individual, but a purchase order had not been raised in these circumstances before the invoice had been received. The Finance Business Partner explained that in some situations a purchase order cannot be raised before an invoice is received (for instance in an emergency) however this is normally very rare.

A goods receipt is required for all purchases and invoices cannot be paid without a goods receipt that matches both the invoice and the purchase order. We selected a sample of 20 invoices and reviewed the system to determine whether a goods receipt had been submitted and that they matched the purchase order and invoice. In all 20 cases, the invoice was not paid until after the goods receipt was recorded on the system and all 20 goods receipts matched the amount recorded on the invoice and purchase order.

All new customers require a new customer form to be completed and signed off by the Lead Business Partner (Finance). We selected a sample of 10 new customers and requested copies of the new customer form to check that this matched the data held on Oracle. In all 10 cases we were provided with a matching form and noted no discrepancies between the new customer form and Oracle.

All credit notes raised must have a completed credit note form which includes sign off by an authorised member of staff. We selected a sample of 20 credit notes and checked to determine whether a credit note form was on file and this had been signed by an appropriate officer as per the authorised signatories list. In all 20 cases we confirmed that a credit note form was on file and had been correctly approved by authorised individuals.

Segregation of duties is clear on the Force's banking system with dual authorisation required for any transaction made. We verified that all users that have access to the system are appropriate, still employed by the Force and have relevant access rights (depending on their job role). We selected a sample of five payments made by the Force and confirmed that they had been requested by one user and approved by another separate user.

We reviewed and walked through the process for accessing the banking system with the Strategic Finance Manager and concluded that only authorised individuals that have been provided with a bank card (provided by NatWest) and unique code can access the Force's bank system. Additionally, once access is granted using the bank card and code, users cannot make payments without approval from another authorised user.

Bank reconciliations are completed monthly by the Treasury Team as part of the month end process. This is then reviewed and approved by the Strategic Finance Manager. We have confirmed the review and approval for the months of June, July and August 2021 for all the Force's bank accounts.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Area: Month-end processes				
Control	The Force operate under a month-end timetable which documents each month end task to be completed and by whom at the month-end Responsibilities are allocated at each step in the month-end procedures document to ensure it is clear who should be reviewing or approving documents.	**Assessment:**		
		Design	✓	
		Compliance	×	
Findings / Implications	The Force have created a month-end procedures document, which provides step-by-step guidance to staff on the completion of the month-end process. This is supported by screenshots from Oracle finance system. The document covers several key areas in the month-end process including budgetary control, closing of the general ledger and cost management. We did note that the procedures document is listed as being last updated in 2018. The Finance Business Partner explained that this was not the case and the document is updated a number of times per year when any improvements to the process are identified and approved. The most recent instance of this being earlier this year (2021). It was also confirmed that no fundamental changes to the process document have been made since 2018. We have raised a suggestion for management to update this document. The process as detailed in the timetable and confirmed by the Finance Business Partner and Accounts Manager is that all ledgers are closed on the first day of month end and variance analysis is completed to determine if there are any discrepancies within the accounts. Returns are completed and submitted to the Lead Business Partner for Finance by each budget holder. The Lead Business Partner for Finance reviews and approves these before putting them into Oracle and providing the data to the Chief Constable. From review of the month end procedures document, we noted that responsibilities for review or approval are clearly outlined at each step in the process.			
Management Action 1	The Force will update the month-end procedure document once it is next reviewed at the end of October 2021	**Responsible Owner:** Head of Financial and Payroll Services	**Date:** 31 October 2021	**Priority:** **Suggestion**

Area: IDEA Testing				
Control	IDEA testing has been completed and the following testing has been completed: <u>Accounts Payable</u> • Identify potential duplicate supplier accounts • Identify multiple supplier accounts with the same bank details • Identify purchase orders above delegated authority thresholds • Identify duplicate payments <u>Accounts Receivable</u> • Identify potential duplicate customer accounts • Identify multiple customer accounts with the same bank details • Identify credit notes or write-offs above delegated authority thresholds • Identify duplicate invoices			
Findings / Implications	We used numerous reports that were printed from the Oracle finance system during our IDEA testing to analyse areas such as duplicate suppliers, purchase order approvals from unauthorised individuals and duplicate payments. Once we completed our IDEA testing, we selected a sample and followed this up with management to determine the scale of the discrepancies. We noted during this sample testing that several discrepancies identified during our IDEA analysis were the result of incorrect data that had been recorded on the reports. For example, the reports suggested that there were numerous duplicate suppliers that had the same bank details but different addresses. Upon review of the Oracle system, we determined that there was only one supplier with one set of bank details but two sets of addresses that corresponded to different offices. Overall, we noted no discrepancies with the Force's controls but did note the discrepancies with the reports printed from the Oracle finance system and that this was providing inaccurate data that did not match Oracle. The Force should review the results of the IDEA testing to determine whether any discrepancies identified require action. More in-depth discussion of the results of the IDEA testing can be seen in Appendix B.			
Management Action 2	The results of the IDEA testing will be reviewed and actioned, where appropriate	**Responsible Owner:** Finance Business Partner	**Date:** 31 December 2021	**Priority:** **Low**

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Area	Control design not effective*		Non Compliance with controls*		Agreed management actions			
					Suggestion	Low	Medium	High
Key Financial Controls	0	(15)	1	(15)	1	1	0	0
Total					**1**	**1**	**0**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: DATA ANALYTICS

The following is a summary of findings from our analytical work which we have discussed with management.

Analytics Findings:

The following is a summary of findings from our data analytics work which we have discussed with management. This has involved us sharing the data analytics spread sheets which detail the findings for further consideration and checking.

For the purpose of our findings, we have used a '*pause*' and '*tick*' approach to highlight at a glance which areas require further investigation following our findings.

Area: Accounts payable – duplicate supplier accounts	
Criteria:	Identify potential duplicate supplier accounts Identify supplier accounts with the same bank account details
Source Data/Reports:	Supplier Listing with Bank Details
Period Covered:	Financial year 2021 / 2022
Testing Undertaken:	Data analysis to identify potential duplicates in each supplier database by reviewing supplier names, supplier vendor IDs, and supplier bank account details. Further sampling of identified discrepancies and discussion with management to determine whether duplicate supplier accounts are legitimate and appropriate within the finance system.
Issues identified:	The supplier listing report contains 2,417 individual supplier entries. We carried out analysis of the supplier listing for duplicate bank account number and sort code number, which resulted in 234 potential duplicate suppliers identified. We selected a sample of 10 sets of suppliers with duplicate bank details from document 1A – supplier duplicates by bank account details and reviewed each set to determine why two suppliers have the same bank account details. In all 10 cases we determined that there was a suitable reason for each set of duplicate bank details: • Two sets of samples were for salary deductions and duplicate bank details had been set up for different deduction reasons (one of the sets for a Sports and Social Association fee alongside a Constabulary Lottery fee). • For one set of duplicates, suppliers have been set for individual barristers but each have the same bank account details. This is to ensure the barristers know which funds are going to which barrister.

Area: Accounts payable – duplicate supplier accounts

- A similar situation occurred with another set of duplicates but for a doctor's practice. No issue was identified.
- Three sets of duplicates are for seized cash payments. We were informed that when seized cash has to be paid back to individuals, they have the option of nominating another individual's bank account. We were provided with the seized cash documents and confirmed this had been correctly set up and no problems had been identified.
- From review of another set of duplicate bank details we noted that one of the suppliers had been end-dated and was no longer active. From review of these two suppliers we noted that one had been bought by the other which was the reason for the duplicate bank details and eventual disabling of the older supplier.
- The remaining two samples reviewed had duplicate supplier details as they were for the same supplier but different sites (and thus different addresses). From review of the Oracle finance system, we determined that two suppliers had not been set up with the same bank details but instead one supplier had been set up with two addresses (each for a different office). We identified that the report that we had been provided had inaccurately marked these as two separate suppliers which is not the case.

We further filtered the 234 potential duplicate suppliers by supplier name, which identified 89 duplicates for supplier name, bank account number and sort code, meaning 145 duplicates with the same bank account details had different supplier names listed.

We selected a sample of five sets of suppliers with duplicate bank details and supplier names from document 1B - supplier duplicates by bank account details and supplier name and reviewed each set to determine the reason for the duplication:

- For four of the five samples we uncovered that there are no duplicate suppliers on the Oracle finance system but instead one supplier with multiple site addresses. This is set up for suppliers that have multiple office sites. We noted that this is a problem with the report rather than the Force's financial control systems.
- For the remaining sample we noted a similar problem however we could not locate the second address on the system. We again believe this to be a problem with the report and not a problem with the Force's finance process.

For the 234 potential duplicate suppliers based on bank account details only, we further ran analysis for duplicate vendor IDs, which resulted in a potential 95 duplicates. This suggests that the Force systems allow for duplicate accounts to one vendor ID.

We selected a sample of five sets of suppliers with duplicate bank details and vendor ID from document 1C - supplier duplicates by bank account details and vendor ID. We reviewed all five samples and concluded that all five had been set up correctly and found only one supplier on Oracle. Again, this is due to a problem with the report provided which was directly printed from the Oracle system. We also found that the vendor ID for two of the suppliers was different to that on the report (though we did not find any problems with regards to duplicate bank details).

We selected a sample of five sets of suppliers with duplicate bank details but different supplier names from document 1D – supplier duplicates by bank account details with different supplier names. For all five sets of samples we noted that a

Area: Accounts payable – duplicate supplier accounts	
	sufficient reason for duplicates had been provided and included two separate departments within one supplier, seized cash and wage deductions.
Overall Conclusion:	Overall, we noted no discrepancies with the Force's control system but did note the discrepancies with the report printed from the Oracle finance system. Reports have been provided to management for further review.

Area: Accounts payable – identify purchase orders above delegated authority thresholds	
Criteria:	Purchase orders are approved only by those authorised to approve orders and within the limits set out within the Force's authorised signatories list.
Source Data/Reports:	XXCPA Orders by Supplier – 01.01.21 to 31.07.21 – Purchase Order Listing Authorised Signatories List – 21.22
Period Covered:	Financial year 2021 / 2022
Testing Undertaken:	Comparison of a summary of purchase order approvers with the Force's authorised signatories list to identify any persons not listed as an authorised signatory. Review of approval of purchase orders over approved thresholds outlined within the Force's authorised signatories list.
Issues identified:	There are 5,875 approved purchase orders on the report provided which includes orders from 1 January 2021 to 31 July 2021. We summarised the list of approved purchase orders by order approver and noted that 56 separate accounts had approved orders. Using collar numbers against each approver, we compared the 56 approvers against the Force's authorised signatories list for 2021 / 2022 and identified that 36 approvers' collar numbers did not appear on the Force's authorised signatories list. We were able to exclude one of the 36 discrepancies as the account pertained to the Lead Business Partner Finance, whose name was listed on the authorised signatories list; however, the collar number had been incorrectly recorded on the list. We expect this to be a typing error. We matched the 35 users not included on the authorised signatories list to the approved orders report, which resulted in 174 records of orders which had been approved by these users, which totalled £138,746. Further sample testing and response is required from management. We selected a sample of five approved purchase orders that have been approved by collar numbers not on the authorised signatories list

Area: Accounts payable – identify purchase orders above delegated authority thresholds	
	and reviewed each to determine the reasoning. We selected these samples from document 2B – POs approved by collar numbers not on authorised signatories list. For all five PO approvals we selected, we confirmed that the collar number on the report had not approved the purchase order. Instead, these individuals had cancelled part or the whole purchase order and an authorised individual had approved the purchase order in the first place. We queried why they had been marked down as approving the PO and were told that the system records when any PO is cancelled and incorrectly marks the individual cancelling the order as approving. The remaining 30 discrepancies require further investigation For the 21 approvers on the authorised signatory list (including the one user with an incorrect collar number), we verified that the remaining 5,701 orders pertained to the 21 approvers. We added the authority limits against each authoriser to 5,701 orders and identified 436 transactions over the authority limits pertaining to four separate users. One of the users did not have their own authority limit but was listed as a delegated authority on the authorised signatories list if the Strategic Finance Manager was on leave and had approved 400 orders. None of these orders exceeded the limit of the Strategic Finance Manager (£2m). The remaining 36 transactions require further investigation. We selected a sample of six purchase orders that were approved but exceeded the authority limit by that individual. We selected this from the document 2D – Orders over authority limit and reviewed each one to determine the reasoning. For four of the six POs we confirmed these had been made by individuals after they had been delegated authority by an individual on the approved signatory list and had not exceeded their authority limit. It was explained that individuals can delegate their authority if they are unavailable for a short period of time (such as illness or annual leave) but this has to be delegated and confirmed through the Oracle system. For the remaining two POs, we noted they had not been approved but due to the system limitations the last individual to edit the PO has been marked as the approver. This is similar to the samples examined from 2B above.
Overall Conclusion:	Overall, these tests noted no discrepancies with the Force's control system. Reports have been provided to management for further review and an action raised to ensure this is undertaken.

Area: Accounts payable – duplicate payments	
Criteria:	Identify instances of potential duplicate payments by comparing invoice received date, payment date, invoice total, supplier name, and number.
Source Data/Reports:	Paid invoices – 01.01.21 – 31.07.21
Period Covered:	2020 / 2021
Testing Undertaken:	Identify instances of potential duplicate payments by comparing invoice received date, payment date, invoice total, supplier name, and number.
Issues identified:	The paid invoices report provided contained 8,513 records. We ran analysis for duplicates based on the following criteria: • invoice received date; • supplier number; • supplier name; • invoice amount; • invoice date; and • invoice number. This analysis produced 2,338 results for paid invoice duplicates. Review of the report identified that there are two period names associated with each paid invoice duplicate: March 2021 (1,169 records) and adjustment 2021 (1,169 records). We expect that the duplicate paid invoices are adjustements for the financial year end. Analysing the paid invoice report based on voucher number only produces the same results totalling 2,338 records. We initially selected a sample of 10 sets of duplicate payments from document 3A – Paid invoices duplicate analysis to review with management on the Oracle system. Upon review of three of these sets of duplicate payments we determined that duplicate payments had not been made and instead there had been a problem with the report. Upon discussion and review with the Finance Business Partner and Accounts Manager we concluded that the report has inaccurately recorded adjustments made for the end of the financial year as duplicate payments and that there has only been one payment made rather than two.
Overall Conclusion:	No discrepancies with the Force's control system have been identified other than the report issues. IDEA reports have been provided to management for further review.

Area: Accounts receivable – duplicate customer accounts	
Criteria:	Identify instances of potential duplicate customer accounts.
Source Data/Reports:	Customer Listing 200921
Period Covered:	2020 / 2021
Testing Undertaken:	We were unable to test for potential duplicate customer accounts using bank account details (as outlined within the agreed scope), as the Force do not record bank account details for customer accounts. Testing was undertaken to determine whether any potential duplicate customer accounts existed based on name and address only. We further undertook analysis for 'fuzzy' duplicates by party name, which identifies any accounts with similar names.
Issues identified:	There are 512 records on the customer listing provided by the Force's finance team. We ran analysis for duplicate customers based on party name and address, which resulted in four potential duplicate customer accounts (consisting of two sets). We reviewed both sets of duplicate customer accounts and noted that for one set of duplicate customers accounts, one of the accounts should have been made inactive as both suppliers were to the same individual. For the second set of duplicate customer accounts, we confirmed that the Oracle system only has one customer and this is instead a problem with the report we were provided. We further conducted analysis on the customer listing for 'fuzzy' duplicates by party name, which identified 52 records of potential duplicate customer accounts. From review of a set of 10 ‘fuzzy’ duplicates by party name all 10 sets consisted of separate customers that had similar but separate customer names. For example, one of the sets of ‘fuzzy’ duplicates cosnusted of the PCC for Lancashire and the PCC for Lincolnshire – two separate organisations.
Overall Conclusion:	No discrepancies were identified during our sample testing. Reports have been provided to management for further review.

Area: Accounts receivable – identify duplicate sales invoices	
Criteria:	Identify potential instances of duplicate sales invoices.
Source Data/Reports:	AR Transactions
Period Covered:	2020 / 2021
Testing Undertaken:	Data analysis to identify potential duplicate sales invoices based on document date, value, and customer.
Issues identified:	There are 495 transactions listed on the accounts receivable report provided. We ran analysis of the transactions by invoice number, date, customer name and amount, which resulted in no identified duplicates. Excluding invoice number from the duplicate analysis criteria, we identified 95 potential duplicates for 16 different customer amounts. We selected a sample of five duplicate sales invoices by amount, customer and date from the document 6A – Duplicate sales invoices by invoice amount, customer and date. We reviewed all five sets of duplicate invoices with management to determine whether the invoices are legitimate and confirmed that: • One set of duplicate invoices had been sent to the same company for the same amount but the bill was for two separate months – December 2020 and January 2021. We confirmed this through review of both invoices. As such this duplication is legitimate. • One set of duplicate sales invoices had been sent to a local council for a legal search fee. We reviewed both invoices and confirmed that these were two separate legal search fees for different individuals and were thus legitimate. • The remaining duplicate sales invoices are with regards to the alarm set-up and monitoring by the Force and, upon review of each invoice, we have confirmed are all for separate sites and are thus accurate.
Overall Conclusion:	From our sample test we identified no discrepancies. Reports have been provided to management for further review.

APPENDIX C: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The internal audit assignment has been scoped to provide assurance on how the Police and Crime Commissioner for Cleveland and the Chief Constable of Cleveland manage the following areas.

Objective of the area under review
The organisations' financial system is appropriately managed to ensure that all financial transactions are accurately recorded.

Scope of the review

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

General

- Financial regulations
- Scheme of delegation / list of budget holders

Month-end processes

- Month-end timetable
- Allocation of responsibilities
- Management of month-end process
- Control account reconciliation preparation and review
- Journal entries and other adjustments

Accounts Payable

- New supplier set up
- Purchase order authorisation
- Goods receipt and invoice authorisation
- Payments to suppliers
- Our work will incorporate the use of Computer Assisted Audit Techniques (CAATs) using the IDEA software package in order to:
  - Identify potential duplicate supplier accounts
  - Identify multiple supplier accounts with the same bank details
  - Identify purchase orders above delegated authority thresholds
  - Identify duplicate payments

Accounts Receivable

- New customer set up
- Receipts from debtors
- Credit notes and write-offs
- Our work will incorporate the use of Computer Assisted Audit Techniques (CAATs) using the IDEA software package in order to:
  - Identify potential duplicate customer accounts
  - Identify multiple customer accounts with the same bank details
  - Identify credit notes or write-offs above delegated authority thresholds
  - Identify duplicate invoices

Treasury Management

- Segregation of duties
- Controls over access to banking systems
- Account reconciliations and review process
- Review and authorisation of payment runs
- Recording of receipts

The following limitations apply to the scope of our work:

- The scope of the work will be limited to those areas examined and reported upon in the areas for consideration in the context of the objectives set out in this review.
- Testing will be completed on a sample basis only, based on transactions from the current financial year.
- We will not review controls over credit cards as agreed with management.
- Our work does not provide assurance on the appropriateness of the transactions entered into, or payments made.
- We will not comment on whether the organisations have achieved value for money from specific transactions.
- Our audit will not cover the broader procurement process.
- Our review will also not include the setting, monitoring and reporting upon budgets relating to the above transactions.
- Our work and report does not provide any assurance on the eventual accuracy at the year end of the current projected outturn or any assurance on the validity and accuracy of any assumptions made in producing the projected outturn.
- Our work does not provide absolute assurance that material error, loss or fraud does not exist.

Debrief held	8 October 2021
Draft report issued	22 October 2021
Revised draft report issued	
Responses received	22 October 2021
Final report issued	22 October 2021

Internal audit Contacts	Dan Harris, Head of Internal Audit
	Philip Church, Senior Manager
	Mike Gibson, Client Manager
	Hollie Adams, Data analytics
	Oliver Gascoigne, Internal Auditor
	James Butler, Internal Auditor
Client sponsor	Chief Finance Officer, OPCC and Deputy Chief Executive
	Chief Constable's Chief Finance Officer
	Lead Business Partner Finance
Distribution	Chief Finance Officer, OPCC and Deputy Chief Executive
	Chief Constable's Chief Finance Officer
	Lead Business Partner Finance

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Police and Crime Commissioner for Cleveland and the Chief Constable of Cleveland**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.