KPMG

Perth and Kinross Council

Interim management report and audit status summary

For the year ended 31 March 2017

17 May 2017

For Audit Committee consideration on 14 June 2017

Contents

About this report

This report has been prepared in accordance with the responsibilities set out within the Audit Scotland's *Code of Audit Practice* ("the *Code*").

This report is for the benefit of Perth and Kinross Council ("the Council") and is made available to Audit Scotland and the Controller of Audit (together "the Beneficiaries"). This report has not been designed to be of benefit to anyone except the Beneficiaries. In preparing this report we have not taken into account the interests, needs or circumstances of anyone apart from the Beneficiaries, even though we may have been aware that others might read this report. We have prepared this report for the benefit of the Beneficiaries alone.

Nothing in this report constitutes an opinion on a valuation or legal advice.

We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the introduction and responsibilities section of this report.

This report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the Beneficiaries) for any purpose or in any context. Any party other than the Beneficiaries that obtains access to this report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through a Beneficiary's Publication Scheme or otherwise) and chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the Beneficiaries.

Complaints

If at any time you would like to discuss with us how our services can be improved or if you have a complaint about them, you are invited to contact Andy Shaw, who is the engagement leader for our services to the Council, telephone 0131 527 6673, email: andrew.shaw@kpmg.co.uk who will try to resolve your complaint. If your problem is not resolved, you should contact Alex Sanderson, our Head of Audit in Scotland, either by writing to him at Saltire Court, 20 Castle Terrace, Edinburgh, EH1 2EG or by telephoning 0131 527 6720 or email to alex.sanderson@kpmg.co.uk. We will investigate any complaint promptly and do what we can to resolve the difficulties. After this, if you are still dissatisfied with how your complaint has been handled you can refer the matter to Russell Frith, Assistant Auditor General, Audit Scotland, 4th Floor, 102 West Port, Edinburgh, EH3 9DN.

Introduction

Purpose of document

In line with our audit strategy we have completed an interim audit. Key activities performed were the testing of a selection of system controls and holding discussions with management to update our understanding and our assessment of the key risks and audit focus areas.

This report provides the Audit Committee with an update on:

1) Significant risks and other focus areas (pages four and five).
2) The results of the control testing (pages six to nine).
3) Best Value approach for years one and two of the five year programme (page 10).
4) Update on prior year recommendations (appendix one).
5) Action plan from results of controls work carried out (appendix two).

Significant risks and other focus areas in relation to the audit of the financial statements as identified in our audit strategy report, dated 24 February 2017:

The significant risks identified were:

— fraud risk from management override of controls;

— fraud risk from income recognition;

— retirement benefits; and

— valuation of property plant and equipment.

The other focus areas identified were:

— presentation of financial statements 'telling the story;

— capital expenditure;

— highway network asset readiness; and

— consolidation of integration joint board.

Acknowledgements

We would like to take this opportunity to thank officers and Members for their continuing help and co-operation throughout our audit work.

Significant risks and other focus areas

Update: significant risks

We outline below updates on significant risk areas included within the Audit Strategy report. We will conclude on these areas in the Annual Audit Report.

Significant risk	Update from strategy
Fraud risk from management override of controls This is an assumed risk from ISA 240 ''The auditors responsibilities relating to fraud in an audit of financial statements'' on which we are required to report.	We have performed controls testing over expenditure, bank reconciliations, budget monitoring, journal authorisation and general IT controls. We did not identify instances where management override of control had occurred. Substantive procedures will be performed during the year end audit, including testing journal entries, assessing accounting estimates and significant transactions that are out with the Council's normal course of business or are otherwise unusual.
Fraud risk from income recognition This is an assumed risk from ISA 240. We consider the fraud risk from other income such as charges or service income to be significant**.**	Testing over higher level controls are set out on page seven and eight, with no exceptions identified. We discussed sources of other income with officers across different services to develop our understanding of the service income which is received. Substantive procedures will be performed during the year end audit. We will consider each source of income and analyse results against budgets and forecasts, performing substantive analytical procedures and tests of details.
Revaluation of property, plant and equipment There is a five year rolling valuations programme with this year's main category being schools. Valuing tangible fixed assets is an inherently judgemental area for all local authorities.	We met with the valuations team and discussed the areas being revalued in 2016-17 as well as reviewing the five year rolling programme. The valuation date is 1 April 2016 as in prior years, with management performing an assessment of whether the valuations as at that date remain appropriate as at 31 March 2017. As part of our year end audit, KPMG's in-house valuer will review the assumptions used to confirm they are reasonable and in line with the Code. A sample of revaluations will be considered in more detail, including the roll forward to 31 March 2017, where all assets need to be held at market value in line with the Code. We will also consider the 31 March 2016 carrying values, as required for our audit of opening balances. We will verify that the revaluation has been correctly disclosed in the accounts and that the accounting entries are correct.

Significant risks and other focus areas

Update: significant risks (cont.)

Significant risk	Update from strategy
Retirement benefits The Council is a member of the Tayside Pension Fund and recognised a defined benefit liability on its balance sheet of £161.821 million as at 31 March 2016. The determination of the net deficit is inherently judgemental given assumptions are used to derive the value.	For our assessment of opening balances, we performed a review of the 2015-16 assumptions provided within the actuary's report. These are in line with the KPMG acceptable range of assumptions for 2015-16. The Council is participating in a pilot scheme which began in February 2016 and requires all data including starters, leavers and changes of hours to be uploaded to an online system. This data is then taken directly from this system by Tayside Pension Fund administrator. This generates a time saving for the team involved in uploading the data and the pilot has so far received positive feedback. We will consider the results of the scheme after the year end. The remaining procedures will be performed during our year end audit. Prior to our field work beginning in July, we will request the agreed assumptions for 2016-17 from management to facilitate consideration and benchmarking by our internal actuary.

Significant risks and other focus areas

Update: other focus areas

Focus area	Update from strategy
Presentation of the financial statements – 'telling the story' CIPFA issued changes to the Code to make the financial statements more understandable and transparent to the reader.	We have discussed with the finance team the revised disclosures and this was presented to Strategy Policy and Resources Committee on 19 April 2017. We will review pro forma financial statements before our field work starts to confirm they are in line with expectations. We will continue to work with officers to ensure the presentational changes made reflect the objectives of the 'telling the story' project.
Highways network assets CIPFA planned to introduce a requirement in the Code to recognise all highway network assets owned by the Council on the balance sheet at depreciated replacement cost. This would result in a material increase in assets.	An announcement was made on 8 March 2017 by the CIPFA/LASAAC Code Board that the introduction of the Highway Network Asset Code into the financial reporting requirements for local authorities would no longer occur. We therefore no longer consider highways network assets to be an area of audit focus.
Capital expenditure There is a capital budget of £100 million for 2016-17 and an inherent risk of delivering projects in line with budget.	We tested controls over capital monitoring and how it is reported to committees, the findings of which are outlined on page nine. We reviewed the capital budget and plan for both 2016-17 and further ahead and will carry out substantive procedures over capital spend at the year end.
Consolidation of the Integration Joint Board ('IJB') The IJB assumed full delegated functions on 1 April 2016. The consolidation of the new entity will have a material impact on the 2016-17 financial statements.	The Council's share of the IJB's results and balances will be included in the Council's consolidated accounts. As this is the first year, we held discussions with officers at any early stage about how the consolidation adjustments will be made and how the results will be treated in the Council's financial statements We presented our audit strategy document to the IJB Audit Committee and have commenced planning work for the IJB audit. We will confirm the accounting treatment and disclosures are in line with guidance in the unaudited financial statements.

Control framework
System controls

In accordance with ISA 330 ''the auditor's response to assessed risks'', we designed and performed tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of relevant controls over the man financial systems. Interim audit testing took place during February and March 2017. Overall we concluded that the control environment is effective.

Test	Description	Results
Bank reconciliations	Bank reconciliations are prepared monthly by the income team and reviewed by a more senior officer. We tested a sample of two months for each of the eight bank accounts to verify they had been authorised and completed on a timely basis.	All reconciliations were completed and authorised as expected. ***Satisfactory***
Budget monitoring	The Council has a robust budget setting process, with involvement of key members of staff. Performance against budget is monitored on a regular basis and formally reported to the Strategic Policy and Resources Committee via the budget monitoring reports. Two months' reports were considered to confirm a sufficient level of detail was presented to and considered by the Strategic Policy and Resources Committee.	Testing confirmed that budget monitoring arrangements are designed, implemented and operating effectively. ***Satisfactory***
BACS authorisation	BACS payment runs must be signed off by an authorised member of the Financial Systems team. A further check is made on individual payments over £75,000. 15 weekly BACS runs were tested to verify they had been approved by an authorised signatory.	All BACS runs had been approved by an authorised officer. ***Satisfactory***
Journals authorisation	A sample of 25 journals were selected and checks carried out to confirm there is segregation of duties exist in who raises and who authorises journal entries. We also considered the back up available for each journal to verify the authoriser could carry out an appropriate review and conclude the journal is correct.	All journals selected were raised and approved by a different officer, however there is no guidance of who can approve journals. ***Recommendation one***

Control framework
System controls (continued)

Test	Description	Results
Payroll	A sample of 16 exception reports were reviewed to confirm investigation and explanation of variances. A sample of two months' BACS runs were reviewed to confirm the payment schedule was reconciled to the net pay analysis report and appropriately authorised. The annual Service Establishment report was reviewed to confirm it has been signed off by each service.	All reports had been reviewed and exceptions investigated. Both BACS runs had been reconciled and authorised The annual report had been reviewed by each service as being accurate. ***Satisfactory***
Cost of services	A sample of 25 purchase orders were tested and agreed to invoice. It was also checked they had been stamped with a goods received note. Procurement testing covered a sample of five contracts. These were checked to verify they had followed the correct tender route based on value. The tender evaluation was also considered.	All purchase orders could be matched to invoice or system for procurement cards. Each contract tested had followed the correct procedures. ***Satisfactory***
Financial reporting	The financial statements are prepared using financial packs from 16 departments. These are consolidated into an extended trial balance and post closing adjustments are then made. We tested controls over the accounts preparation process in relation to these packs. We tested a sample of two packs to verify they had been signed as prepared as well as signed by the person authorising. A management checklist is also required to be completed for each service.	While some of the packs had been authorised, one of the packs had not and when the sample size was increased more were identified that had not been authorised. In several cases the management checklist was incomplete or missing. ***Recommendation two***

Control framework
System controls (continued)

Test	Description	Results
Capital expenditure	Capital expenditure is monitored throughout the year via capital monitoring reports which are reported to the Strategic Policy and Resources Committee each month. Two reports were reviewed to confirm a sufficient level of scrutiny took place over variances and reasons were given for slippage and movements from budget.	Variances in capital projects are reviewed in sufficient detail. ***Satisfactory***
Polices and procedures	Staff have access to a number of polices and procedures through the Council's intranet system, 'eric'. Policies include the Communications Security Policy, Conflict of Interest Procedure and the Employee Code of Conduct. We carried out a review of the key documents to ensure they covered all expected information and were updated within the prescribed timeframe.	All expected polices and procedures were available to staff on eric. Out of date polices were found on the system, which have been superseded. The most recent policy in some cases was from 2010 with no evidence of review since this date. The Whistleblowing policy did not contain some best practice areas identified in the Public Concern at Work Whistleblowing code of practice 2013. ***Recommendation three***
General IT controls	We performed testing over key IT systems will place reliance on as part of our audit. This included Integra and Resource Link and considered: — programme changes were authorised and requested by the appropriate officers; — user access was authorised over starters and amendments; — leavers access was removed timeously; and — appropriate users were assigned system administrator user access.	Overall controls were found to be operating effectively within IT, however one weakness was identified; Three leavers had not had their access removed from the Council network at the time of testing. It was however noted they had not accessed the system. ***Recommendation four***

Wider Scope and Best Value

The Code of Audit Practice sets out four audit dimensions which, alongside Best Value, set a common framework for all audit work conducted for the Accounts Commission. These areas are: governance and transparency, financial management, financial sustainability and value for money. During our interim audit we considered these areas and will conclude our assessment in our Annual Audit Report. We provide an update below of work carried out so far on Best Value.

Area	Audit update
Best Value	In year one (2016-17), in line with guidance from the Accounts Commission, we will report on the areas of Financial Governance and Resource Management and Financial Planning. This will be concluded in our Annual Audit Report. We have held planning discussions with officers to obtain an understanding of the Council's approach to Best Value and how this is embedded within the Council's culture. We have reviewed publically available evidence across these two Best Value areas and discussed with management, requesting further support or explanation for us perform the review of Best Value. We will continue to gather information and meet with officers to build or knowledge of Best Value in order to conclude on the two year one areas in our annual audit report. In year two (2017-18) we will consider the Best Value areas of Leadership, Scrutiny and Governance and Improvement.

KPMG

Appendices

Appendix one

Prior year recommendations

This section provides an update on prior year external audit recommendations, to determine whether they have been addressed. The table below summarises the recommendations made during the 2015-16 by Audit Scotland.

Original finding and risk	Recommendation	Original management actions	Status
Treasury management			
Only authorised amendments to standing data (e.g. bank account details) should be processed. Within the treasury management section these changes have been rare however there are no system controls to ensure that only authorised changes to standing data are processed and therefore fraudulent changes could be made. **Risk:** Payments are made to the wrong individuals.	A review of changes to standing data should be evidenced to confirm only authorised amendments are made.	There are procedures to ensure that requests from third parties to change their bank details for future payments are genuine. In the case of new counterparties being used for the first time, external confirmation of the bank account details are supplied to the Income Team with the payment request, providing evidence that the payment request and bank details are genuine and correct. Such evidence could be in the form of the counterparties own deal confirmation, and/or the brokers confirmation (where applicable). There are no available controls within the Treasury Management system ('STM) to prevent changes to counterparty bank details. PSTM only gives two levels of access, read-only or full access rights, and all staff involved in Treasury need full access rights. However PSTM does maintain an audit log so transactions on the system can be reviewed. The Senior Accountant will liaise with the systems suppliers to determine whether improved access controls can be implemented. **Implementation date: June 2016**	**Implemented but with further improvement suggested** A systems administrator has been set up who is independent from the treasury team and is the only individual who can amend bank details. There is no procedure for when the systems administrator is unavailable. It is recommended that another person is given this access as a contingency. **Implementation date: April 2017**

Prior year recommendations (continued)

Original finding and risk	Recommendation	Original management actions	Status
Trade receivables			
Authorised signatories are maintained to ensure only appropriate credit notes are processed. During the testing Audit Scotland noted two officers had been authorising credit notes although their authorisation limits excluded credit notes. Neither the officers authorising nor the officers processing the credit notes were aware of this omission. The authorised signatory forms have subsequently been amended. **Risk**: Errors/manipulation is undetected	Officers should confirm that credit notes are appropriately authorised prior to processing.	As noted the remedial action required to rectify this instance has been undertaken to resolve the operational issue. In terms of strengthening our internal controls, the possibility of creating a standard Integra e-form is being investigated that, it is hoped, will allow a user to raise a credit note and automatically workflow the authorisation to a nominated officer with a credit note authorisation profile. **Implementation date: 31 August 2016**	**Ongoing** As of October 2016, an Integra e-form has been piloted with Health and Social care, to replace the previous manual system. In the new system, a request for a credit note is raised electronically on Integra: the form includes selecting an authoriser from a pre-set drop down list. The authoriser is notified by email of the request to electronically approve the credit note on Integra. It is hoped that the e-form will be implemented across the organisation in Summer 2017. We will follow this up in 2017-18 to assess the impact of the form being rolled out on the control environment. **Implementation date: August 2017**

Prior year recommendations (continued)

Original finding and risk	Recommendation	Original management actions	Status
SWIFT			
To ensure the validity of information in the SWIFT system various exception reports are considered by officers. For instance short break and crisis admissions with no end date; client died-service not ended etc. Audit Scotland's sample covered five weeks and included forty six exception reports within this period, however, thirty of these exception reports were either unavailable or there was no evidence of review. **Risk**: Errors in or manipulation of the SWIFT system is undetected.	Exception reports should evidence the checks undertaken and should be retained for the appropriate period.	Although there were some reports which showed no evidence of review, our validation reports work on an exceptions basis so blank reports will not show any evidence of having been reviewed. If any cases highlighted on a validation report are not corrected when the report is reviewed, they would continue to show on future reports until they have been. Going forward however, all validation reports will be printed, signed, dated and stored for a period of 18 months. This will ensure that evidenced reports are available for any future audit reviews. **Implementation date: 9 May 2016**	**Implemented** All exception reports are now being printed, signed and dated and stored in hard copy. It is recommended that to reduce the amount of staff time and printing required and improve the efficiency within the department, exception reports are stored electronically. ***Recommendation five***
Non domestic rates			
Accuracy checks on the processing of changes to the NDR system are run daily and officers undertake checks on a number of the claims. As at April 2016, however, the accuracy checks from December 2015 had yet to be undertaken. **Risk**: Errors in or manipulation of the NDR system is not detected timeously.	Accuracy checks should be undertaken timeously.	The audit finding is accepted and understood. Renewed effort will be made to rectify this matter by ensuring the outstanding checks are completed and ongoing checks are carried out timeously. **Implementation date: June 2016**	**Implemented** Checks are now being completed on time and now more accurately reflect the circumstances of the service (i.e. new staff or those returning from long term absence have their work checked more than others).

Prior year recommendations (continued)

Finding(s) and risk(s)	Recommendation(s)	Orignal management actions	Status
Non domestic rates			
State Aid is any advantage granted by public authorities through state resources on a selective basis to any organisations that could potentially distort competition and trade in the European Union. There is a de-minimis of 200,000 euros (or Sterling equivalent) for State Aid purposes that can be granted over a rolling three year period. Audit Scotland's testing highlighted one case in relation to renewable energy generation relief where an award was granted on the basis of a three year fixed period rather than a three year rolling period. This resulted in a payment in excess of the State Aid de minimus of approximately £0.022 million. **Risk**: The council fails to comply with State Aid requirements and may be unable to recover the costs from the recipient.	State Aid for renewable energy requires to be considered on a three year rolling basis to ensure breaches are avoided.	Officers will: — seek advice from the State Aid team in order to properly deal with these instances; — ensure these cases are reviewed annually; and — enter a diary event date on the Northgate System. **Implementation date: ongoing**	**Implemented** As a result of the matter in 2015-16, a training programme has been rolled out to appropriate staff to make them aware of the State Aid regulations. This includes how to calculate the total award given, to assess if this breaches the de minimis.

Appendix two

Current year action plan

This is the current year action plan based on the findings from our controls work. We set out the finding, risk and recommendation. We provide a priority grading for recommendations which is set out below;

Priority rating for recommendations		
Grade one (significant) observations are those relating to business issues, high level or other important internal controls. These are significant matters relating to factors critical to the success of the Council or systems under consideration. The weaknesses may therefore give rise to loss or error.	Grade two (material) observations are those on less important control systems, one-off items subsequently corrected, improvements to the efficiency and effectiveness of controls and items which may be significant in the future. The weakness is not necessarily great, but the risk of error would be significantly reduced if it were rectified.	Grade three (minor) observations are those recommendations to improve the efficiency and effectiveness of controls and recommendations which would assist us as auditors. The weakness does not appear to affect the availability of the control to meet their objectives in any significant way. These are less significant observations than grades one or two, but we still consider they merit attention.

Finding and risk	Recommendation	Agreed management actions
1. Journals review		**Grade three**
Controls testing was performed over journals by selecting a sample of 25 journal entries and checking the review. In all cases a different officer had reviewed the journal compared to who had raised it, therefore the segregation of duties control is operating effectively. However there is no documentation of who has the authority to review journals, therefore we cannot assess it will always be an officer with sufficient experience who is carrying out this review.	It is recommended that controls over journals are strengthened: — the general ledger procedures manual should be updated to give clearer description of who can review journals. This should include a description of officer grade and journal value. — individuals involved in preparing and reviewing journals should be reminded of the procedures manual and the importance of complying with this.	**ACCEPTED** **Management response** General ledger manual will be updated to provide guidance on the roles and responsibilities of officers involved in checking journals. It shall provide a checklist for authorisers and examples of which officers should be reviewing / approving journals. **Implementation date** 30 September 2017 **Responsible officer** General Ledger Controller

Current year action plan (continued)

Finding and risk	Recommendation	Agreed management actions
2. Service pack authorisation		**Grade two**
The financial statements are prepared using information from a number of departments. There are five service packs from the main divisions with an additional 11 corporate packs such as loans fund and general fund. These packs are consolidated into an extended trial balance and post closing adjustments are then made to derive the final accounts. The service packs are required to be signed by a preparer and authoriser, who is responsible for checking that these are complete and accurate. A management checklist is also required to be prepared for service packs, to show which checks the authoriser has performed. From testing carried out on the 2015-16 service and corporate packs, we identified three that had not been authorised, while several had a missing or incomplete management checklist. In an number of cases questions had been raised on the management checklist but no follow up had been documented and it is unclear if the issue had been resolved. There is a risk that the information used to prepare the financial statements is not complete or accurate of fully reconciled to supporting documentation.	It is recommended the controls over the authorisation of service packs are strengthened by: — ensuring all packs are signed as having been reviewed by the responsible officer for that service; — completing management checklists for each service pack, marking any questions that are not applicable as such, rather than leaving them blank; — reminding staff which, if any, corporate packs require a management checklist. — ensuring questions raised on the management checklist show evidence of follow up to ensure issues are resolved and there is a clear audit trail.	**ACCEPTED** **Management response** An instruction will be issued to all reviewers to ensure that accounts pack include an Accounts Preparation Certificate which is completed by preparers and reviewers. The instruction will also remind officers of the importance of completing the managers checklist and documenting issues that are identified during the review process **Implementation date** Complete – 9 May 2017 **Responsible officer** Chief Accountant

Current year action plan (continued)

Finding and risk	Recommendation	Agreed management actions
3. Checklist for updating polices		**Grade three**
Polices and procedures are held on the Council's intranet which is available to all staff. From a review of key policies we identified that a number had not been updated on a timely basis. Two versions of the communications security policy were found. The most up to date version of this policy was dated 2010, however it states it is required to be be reviewed every three years. The most up to date whistleblowing policy is not easily accessible to staff and also does not contain all information outlined in the Public Concern at Work's whistleblowing code of practice. There is a risk employees access policies and procedures which are not relevant to the current risk environment or contain out of date information therefore causing error or breach of laws and regulations.	It is recommended that: — a review is carried out of existing polices on the intranet and any old or superseded policies are removed; — the whistleblowing policy is made available on the intranet and is updated to contain all items required by the whistleblowing code of practice; and — a checklist should be kept of the key polices and when these were last updated, with evidence of review within the required timescale.	**ACCEPTED/NOT ACCEPTED** **Management response** Services will be reminded of the need to ensure all policies are reviewed in line with agreed timescales, to document the review and to amend the date of policy to reflect the review. Services will also be reminded of the need to ensure that old or superseded policies on the intranet are either clearly marked as such or are removed from the intranet. The whistleblowing policy is available on the intranet and is maintained appropriately. Consideration will be given to creating and maintaining an appropriate checklist of Council policies. **Implementation date** 30 May 2017 **Responsible officer** Information Compliance Manager

Current year action plan (continued)

Finding and risk	Recommendation	Agreed management actions
4. GITCs - leavers		**Grade three**
During testing of general IT controls it was identified that some staff members who had left the Council had not had their user access removed (three from a sample of 16). Whilst there was evidence that these individual staff members had not accessed the system since their departure date, it highlights a control deficiency over removal of user access rights. The risk of unauthorised access to Integra and Resource Link was countered by mitigating controls at the system specific level. However there is a risk that former members of staff may access the Council's computer systems after their departure date. Depending on their access levels they would therefore potentially be able to make fraudulent or malicious use of council IT systems.	It is recommended that controls over the removal of leaving staff members' access are strengthened: — monthly reports of all leavers received from HR should be printed off or saved electronically; — each leaver on the report should be marked as having had their access removed; — the report should be signed and dated by the person performing the control to confirm completion, and — a designated member of IT management should regularly review the existence of the monthly leaver reports to confirm the control has been performed.	**ACCEPTED** **Management response** From discussion with the IT department the leavers report was not being processed correctly during the first half of 2016. This was due to staffing issues and has now been corrected. Our testing of January 2017 confirmed all leavers had been removed. **Implementation date** Complete – April 2017 **Responsible officer** Corporate IT Manager

Current year action plan (continued)

Finding and risk	Recommendation	Agreed management actions
5. SWIFT exception reports efficiency		**Grade three**
Exception reports are produced each week on data held in the SWIFT system relating to residential care homes. At present, and in line with prior year recommendation, all 14 of these reports are printed, dated, signed and held for 18 months. While this is helpful for audit evidence it creates a large amount of paperwork and takes up officers time in printing and documenting these reports. There is an opportunity to use staff time more efficiently.	It is recommended that a control sheet is put in place listing the 14 exception reports and whether any exceptions were noted. If there were no exceptions for a specific report this should be documented, initialled and dated by the officer who checked the report. An exception report with zero entries does not have to be printed, however this should still be held electronically. For cases where exceptions do exist these could be evidenced and stored electronically.	**ACCEPTED** **Management response** The service accept the recommended changes to the recording of SWIFT exception reports and the efficiency that the changes will bring. **Implementation date** Complete - April 2017 **Responsible officer** Business and Resource Manager

The contacts at KPMG in connection with this report are:

Andy Shaw

Director

Tel: 0131 527 6673

andrew.shaw@kpmg.co.uk

Michael Wilkie

Senior Manager

Tel: 0141 300 5890

michael.wilkie@kpmg.co.uk

Fiona Bennett

Assistant Manager

Tel: 0141 228 4229

fiona.bennett@kpmg.co.uk