cutting through complexity™

Interim Audit Report 2014/15

Wiltshire Council

June 2015

Contents

The contacts at KPMG in connection with this report are:

Darren Gilbert
Director
KPMG LLP (UK)

Tel: 0292 046 8205
darren.gilbert@kpmg.co.uk

Tara Westcott
Senior Manager
KPMG LLP (UK)

Tel: 0117 905 4358
tara.westcott@kpmg.co.uk

Adam Bunting
Assistant Manager
KPMG LLP (UK)

Tel: 0117 905 4470
adam.bunting@kpmg.co.uk

Page

Report sections

Appendices

This report is addressed to the Authority and has been prepared for the sole use of the Authority. We take no responsibility to any member of staff acting in their individual capacities, or to third parties. The Audit Commission issued a document entitled Statement of Responsibilities of Auditors and Audited Bodies summarising where the responsibilities of auditors begin and end and what is expected from audited bodies. We draw your attention to this document which is available on Public Sector Audit Appointment's website (www.psaa.co.uk).

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

We are committed to providing you with a high quality service. If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Darren Gilbert, the engagement lead to the Authority, who will try to resolve your complaint. If you are dissatisfied with your response please contact the national lead partner for all of KPMG's work under our contract with Public Sector Audit Appointments Limited, Trevor Rees (on 0161 246 4000, or by email to trevor.rees@kpmg.co.uk). After this, if you are still dissatisfied with how your complaint has been handled you can access PSAA's complaints procedure by emailing generalenquiries@psaa.co.uk, by telephoning 020 7072 7445 or by writing to Public Sector Audit Appointments Limited, 3rd Floor, Local Government House, Smith Square, London, SW1P 3H.

Introduction

This document summarises the key findings arising from our work to date in relation to the audit of the Authority's 2014/15 financial statements.

Scope of this report

This report summarises the key findings arising from:

- our interim audit work at Wiltshire Council ('the Authority') in relation to the Authority's 2014/15 financial statements;
- our interim audit in relation to the 2014/15 financial statements for the Wiltshire Pension Fund ("the Pension Fund"); and

This report does not cover our 2014/15 value for money (VFM) conclusion. Our work in relation to this will be undertaken during June 2015.

Financial statements

Our *External Audit Plan 2014/15*, presented to you in March 2015, set out the four stages of our financial statements audit process.

During January to April 2015 we completed our planning and control evaluation work. This covered:

- review of the Authority's general control environment, including the Authority's IT systems;
- testing of certain controls over the Authority's key financial systems;
- assessment of the internal audit function; and
- review of the Authority's accounts production process, including work to address prior year audit recommendations and the specific risk areas we have identified for this year.

VFM conclusion

Our *External Audit Plan 2014/15* explained our risk-based approach to VFM work, which follows guidance provided by the Audit Commission (now replaced by Public Sector Appointments Authority Ltd), and detailed our initial risk assessment.

We will complete our work in response to the specific risks identified during our final visit in June. The results of this work will be reported in our *ISA 260 Report 2014/15*.

Structure of this report

This report is structured as follows:

- **Section 2** summarises the headline messages.
- **Section 3** sets out our key findings from our interim audit work in relation to the 2014/15 financial statements.

Our recommendations are included in **Appendix 1**. We have also reviewed your progress in implementing prior recommendations and this is detailed in **Appendix 2**.

Acknowledgements

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

Headlines

This table summarises the headline messages. The remainder of this report provides further details on each area.

Organisational and IT control environment	Your organisational control environment is effective overall. Progress in improving the overall IT control environment has continued to be made during this period with one of the three prior year recommendations being fully implemented, and the priority one recommendation now reduced to a priority two recommendation. The prior year priority one recommendation was in relation to the limiting and monitoring of privileged access within the SAP system. Although CGI still hold the same level of access, further controls have been introduced within the period which mitigate the risk by allowing the Authority to confirm that there has been no unauthorised access during the period. As a result of enabling this control, we are able to fully rely on your IT control environment. A small number of additional issues have been identified in relation to the Authority's disaster recovery processes and the maintenance of access to the SAP system. Further details are provided in **Appendix 1**.
Controls over key financial systems	In relation to those controls upon which we will place reliance as part of our audit, the key financial systems are generally sound. Despite this, Internal Audit identified weaknesses in relation to the controls in operation around starters and leavers. As a result of this we will not be able to place reliance on these controls and additional substantive testing will be necessary at year end.
Review of internal audit	During the year we have met regularly with SWAP in order to maintain a close working relationship and to build on our joint working protocol. In relation to our work on the Authority's financial controls, we were able to place reliance upon the work of Internal Audit in those areas where we are intending to rely upon controls. Working papers produced by Internal Audit were of an appropriate standard, and were supported by the required evidence. However, we did identify one area where further improvement could still be made in relation to the clarity of documentation. Full details are set out page 6. We have again placed reliance on the work of Internal Audit in respect of IT controls where this has been performed. Whilst the scope of work undertaken by SWAP was subject to limitations that had been communicated to us prior to the commencement of our work and was incorporated into our planned procedures.
Accounts production and specific risk areas for the Authority	The Authority's overall process for the preparation of the financial statements is strong. The Authority has taken the key risk areas we identified seriously and made good progress in addressing them. However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.
Pension Fund audit	We have completed our interim audit in relation to the Pension Fund's 2014/15 financial statements and have identified no issues to report at this stage.

Organisational control environment

Your organisational control environment is effective overall.

Work completed

Controls operated at an organisational level often have an impact on controls at an operational level and if there were weaknesses this would have implications for our audit.

We obtain an understanding of the Authority's overall control environment and determine if appropriate controls have been implemented. We do not complete detailed testing of these controls.

Key findings

We consider that your organisational controls are effective overall.

Our findings in relation to the IT control environment reflects the results of our work undertaken on the general IT controls in operation with regard to each of the Authority's key IT systems.

During the year the Authority has continued to make progress in relation to the adequacy of IT Controls. Despite this we identified a number of new areas where further improvements could be made. These are identified on the following page and in **Appendix 1**.

Aspect	Assessment	
	2014/15	2013/14
Organisational controls:		
Management's philosophy and operating style	3	3
Culture of honesty and ethical behaviour	3	3
Oversight by those charged with governance	3	3
Risk assessment process	3	3
Communications	3	3
Monitoring of controls	3	3
IT control environment	2	2

Key:		
	1	Significant gaps in the control environment.
	2	Deficiencies in respect of individual controls.
	3	Generally sound control environment.

IT control environment

Your IT control environment is effective overall and improvements over the IT control environment have continued to be made.

Work completed

The Authority relies on information technology (IT) to support both financial reporting and internal control processes. In order to satisfy ourselves that we can rely on the use of IT, we test controls over access to systems and data, system changes and maintenance, system development and computer operations over the SAP and Civica environments.

In completing this work, we have been able to rely on internal audit's reviews of some of the SAP system controls. As a result of an agreed limitation to the scope of SWAP's work however, we have undertaken additional testing of both the SAP and Civica systems.

In reviewing Internal Audit's work it was identified that a number of control weaknesses had been identified, however, at the time of our audit these issues had not been discussed with officers and formally reported within an Internal Audit Report. Issues identified by Internal Audit include:

- Improvements required within the processes for managing operational changes to the SAP system including the completeness of documentation being retained.
- The reviews of SAP user roles within Finance and Procurement functions have not been completed.

As these weaknesses will be reported by SWAP, we are not repeating any of them within this report to prevent the duplication of recommendations.

Key findings

We again note that further improvements have been made in the current year in respect of the IT control environment, specifically in relation to the previous 'Access to systems and data' priority one recommendation that has been raised over the last few years.

Whilst the risk previously identified still exists, the physical relocation and in-sourcing of responsibility for the SAP environment to the Authority has facilitated the implementation of mitigating controls that have resulted in the Authority having assurance that no unauthorised use of these high privilege accounts occurred during the relevant period. Despite this, we identified a number of ongoing issues still to be addressed as set out in **Appendix 2**.

Due to the issues highlighted by Internal Audit, we have again rated the processes in relation to "System changes and maintenance" as having deficiencies in respect of individual controls.

Although the overall number of recommendations requiring action, including outstanding prior year recommendations, has increased from three to five, the degree of risk attached to these recommendations has reduced, with no Category 1 issues identified.

We consider that, despite the issues identified, we are able to rely upon the Authority's IT control environment. In addition, as a result of improvements made during the year, we will not need to undertake additional testing to compensate for SAP deficiencies as has been the case in prior years.

Recommendations are included in **Appendix 1**.

Aspect	Assessment	
	2014/15	2014/13
IT controls:		
Access to systems and data	❷	❶
System changes and maintenance	❷	❷
Development of new systems and applications	❸	❸
Computer operations and end-user computing	❸	❸

Key:
❶ Significant gaps in the control environment.
❷ Deficiencies in respect of individual controls.
❸ Generally sound control environment.

Review of internal audit

Following our assessment of Internal Audit, we were able to place reliance on their work (as per agreed coverage) on both the key financial and IT systems.

Background

The United Kingdom Public Sector Internal Audit Standards ("PSIAS") apply across the whole of the public sector, including local government. These standards are intended to promote professionalism, quality, consistency and effectiveness of internal audit across the public sector. Additional guidance for local authorities is included in the Local Government Application Note on the PSIAS.

Work completed

The scope of the work of your internal auditors and their findings informs our audit risk assessment.

We work with your internal auditors to assess the control framework for certain key financial systems and seek to rely on any relevant work they have completed to minimise unnecessary duplication of work. Our audit fee is set on the assumption that we can place full reliance on their work.

Where we intend to rely on internal audit's work in respect of the Authority's key financial systems, auditing standards require us to complete an overall assessment of the internal audit function and to evaluate and test aspects of their work.

The PSIAS define the way in which the internal audit service should undertake its functions. Internal audit completed a self-assessment in 2011/12 against the standards set out in this document in advance of them becoming applicable and as a result developed an action plan against which they have been working to ensure full compliance. They are planning to begin an updated self assessment in the upcoming months.

We reviewed internal audit's work on the key financial systems and re-performed a sample of tests completed by them.

Key findings

Based on the self-assessment performed by internal audit, our assessment of their files, attendance at Audit Committee and regular meetings during the course of the year, we have not identified any significant issues which would indicate internal audit are not compliant with the PSIAS.

We did not identify any significant issues with internal audit's work and are pleased to report that we were able to place reliance on internal audit's work on a number of financial systems.

However, there is one ongoing improvement that could be made to further enhance the quality of internal audit's work:

- Documentation of Mitigating Controls: Internal audit's work programmes set out the expected controls which are to be tested as part of any individual review. Where the expected control was not in place, appropriate work was undertaken in order to identify and test mitigating controls. In such instances, however, greater clarity of documentation was required in relation to how the alternative controls identified provided assurance over the same risk areas.

This matter has been discussed with SWAP officers and we have included a recommendation in **Appendix 1**.

We are mindful that internal audit try to cover testing that covers the whole of the Authority's financial year and in some instances because of the timing of their work, the close down meetings or draft internal audit reports have not been finalised in time for our interim work.

As a result of this there is a potential that findings will be revised. Where this happens, additional work may be required to meet our own requirements. No such work has been required to date, and we will liaise with the Authority in the event that such a need arises.

Controls over key financial systems

The controls over the key financial systems are generally sound, with the exception of Payroll which requires limited improvements required.

Internal audit have raised a number of recommendations during the year. Whilst the majority of these have no impact on our audit, weaknesses in the payroll system will need to be considered as part of our final visit.

Work completed

We review the outcome of internal audit's work on the financial systems to influence our assessment of the overall control environment, which is a key factor when determining the external audit strategy.

We also work with your internal auditors to update our understanding of some of the Authority's key financial processes where these are relevant to our final accounts audit.

Where we have determined that this is the most efficient audit approach to take, we test selected controls that address key risks within these systems. The strength of the control framework informs the substantive testing we complete during our final accounts visit.

Our assessment of a system will not always be in line with the internal auditors' opinion on that system. This is because we are solely interested in whether our audit risks are mitigated through effective controls, i.e. whether the system is likely to produce materially reliable figures for inclusion in the financial statements.

Key findings

Based on our work, and the work of your internal auditors, in relation to those controls upon which we will place reliance as part of our audit, the key financial systems are generally sound.

However, internal audit have identified a number of issues within starter and leaver payroll controls. In the sample of 25 there were five starter forms and four leaver forms unavailable to review. Whilst there were mitigating controls which provided assurance for some of the issues identified (in the form of evidenced approval of recruitment for the posts in question) they do not cover the full range of deficiencies identified. As a result we are not able to rely upon these payroll controls for our Audit.

Recommendations in relation to the weaknesses identified have already been raised by Internal Audit and as a result will not be repeated in this report.

Financial system	Assessment	
	2014/15	2013/14
Property, Plant and Equipment	❸	❸
Payroll costs	❷	N/a
Cash and Cash Equivalents	❸	❸
Pension Costs and Liabilities	❸	❸

Key:		
	❶	Significant gaps in the control environment.
	❷	Deficiencies in respect of individual controls.
	❸	Generally sound control environment.
	N/a	Not tested

Accounts production process

The Authority's overall process for the preparation of the financial statements is strong.

Accounts production process

We issued our Accounts Audit Protocol to the Associate Director (Finance) on 24 February 2015. This important document sets out our audit approach and timetable. It also summarises the working papers and other evidence we require the Authority to provide to support our audit work.

We continue to meet with the finance team on a regular basis to support them during the financial year end closedown and accounts preparation.

Key findings

We consider that the overall process for the preparation of your financial statements is strong. During 2013/14, the timetable for the production of the financial statements was been brought forward by one month. The finance team managed well despite the additional pressures this caused.

Our *ISA 260 Report 2013/14* included one recommendation relating to the financial statements process. This recommendation related to the assurance gained over those assets that are not revalued as part of the rolling valuation programme. The progress made in relation to this recommendation will be assessed during our final visit.

Please note we have not specifically reviewed the accounts production process for the Pension Fund at this point in our work.

Specific audit risk areas

The Authority has a good understanding of the key audit risk areas we identified and is making progress in addressing them.

However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

Work completed

In our *External Audit Plan 2014/15*, presented to you in March, we identified the key audit risks affecting the Authority's 2014/15 financial statements.

Our audit strategy and plan remain flexible as risks and issues change throughout the year. To date there have been no changes to the risks previously communicated to you.

We have been discussing these risks with finance officers as part of our quarterly meetings. In addition, we will seek to review relevant workings and evidence, and agree the accounting treatment, as part of our final work.

Key findings

The Authority has a clear understanding of the risks and making progress in addressing them. However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

The table on the following page provides a summary of the work the Authority has completed to date to address these risks.

Specific audit risk areas (continued)

The Authority has a good understanding of the key audit risk areas we identified and is making progress in addressing them.

However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

Key audit risk	Issue	Progress
Accounting for Local Authority Maintained Schools	LAAP Bulletin 101 *Accounting for School Assets used by Local Authority Maintained Schools* issued in December 2014 has been published to assist practitioners with the application of the Code in this respect. The challenges relate to school assets owned by third parties such as church bodies and made available to school governing bodies under a variety of arrangements. This includes assets used by Voluntary-Aided (VA) and Voluntary-Controlled (VC) Schools as well as Foundation Schools. Authorities will need to review the agreements under which assets are used by VA/VC and Foundation schools and apply the relevant tests of control in the case of assets made available free of charge, or risks and rewards of ownership in the case of assets made available under leases. This is a key area of judgement and there is a risk that Authorities could omit school assets from, or include school assets in, their balance sheet. Particular risks surround the recognition of Foundation School assets which may or may not be held in Trust. Authorities should pay particular attention to the nature of the relationship between the Trustees and the school governing body to determine whether the school controls the Trust and the assets should therefore be consolidated into their balance sheet.	As at the time of our interim visit, the Authority's review and valuation exercises were still ongoing. As a result, this matter will be revisited as part of our final visit in June. As part of out year end work we will review the assessments undertaken by the Authority is order to ensure that they comply with the requirements of the LAAP Bulletin and any resulting transactions have been accounted for appropriately.

Appendix 1

Key issues and recommendations

We have given each recommendation a risk rating and agreed what action management will need to take.

The Authority should closely monitor progress in addressing specific risks and implementing our recommendations.

We will formally follow up these recommendations next year.

Priority rating for recommendations		
❶ ***Priority one***: issues that are fundamental and material to your system of internal control. We believe that these issues might mean that you do not meet a system objective or reduce (mitigate) a risk.	❷ ***Priority two***: issues that have an important effect on internal controls but do not need immediate action. You may still meet a system objective in full or in part or reduce (mitigate) a risk adequately but the weakness remains in the system.	❸ ***Priority three***: issues that would, if corrected, improve the internal control in general but are not vital to the overall system. These are generally issues of best practice that we feel would benefit you if you introduced them.

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
1	❷	**Disaster Recovery Planning and Risk Management** Currently there is only a very high level Disaster Recovery (DR) Plan in place which was originally developed in 2013 and has not been updated since, despite the recent changes to the Authority infrastructure. The current plan is not scenario based and only provides very general guidance for DR incidents. No DR rehearsals or tests have been carried out in the financial year. The absence of a detailed DR Plan creates an enhanced risk that, in the event of a system failure, the Authority's response will be either incomplete or inefficient. This may result in systems unavailability being protracted. The issue was discussed with management during the audit who recognized the risk posed by a lack of effective DR planning and testing but named resource constraints as reason for the lack of them. **Recommendation** A detailed DR plan should be developed, implemented and regularly tested.	We agree and endorse this recommendation and would say that we take DR very seriously. Whilst we do have an emergent DR Plan, we recognise that it is not complete and will seek to firm it up with scenarios and responses as appropriate and in line with the recommendations outlined in ISO22301. This will be a continuing process and so has no end date **Responsible Officer:** Steve Grieshaber (Acting Head of Service: ICT Infrastructure) **Due Date:** Ongoing

Appendix 1

Key issues and recommendations *(continued)*

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
2	❸	**Removal of user access - SAP** Testing of 100% of the leavers identified two accounts (SHAWDA and QUINTOJO) that had been accessed four and eight days after the users’ leave date as recorded by HR. These accounts had been locked at the time of the audit and neither of them had access to financial or privileged transactions. For account SHAWDA, a service request to remove the account was received, detailing the user’s leave date as different than the one outlined by HR. Based on the date included on the service request, the user would not have been able to log on after their leave date. For user QUINTOJO no service request was received but the account was locked as a result of mitigating controls. Where user accounts are not terminated on a timely basis there is a risk of unauthorised access to the Authority’s IT systems. This is partially mitigated, however, by the effective operation of network level access controls. **Recommendation** The Authority should reiterate the importance of timely service requests to remove accounts of leavers to relevant officers.	We agree and endorse this recommendation and would reiterate that it was the compensating controls developed within ICT which picked up these late notifications from the business. The recommendation to reiterate the importance of timely notification of leavers has been escalated to the appropriate Associate Director via ICT Head of Service. This recommendation is therefore complete. **Responsible Officer:** Jason Atkinson (Senior Applications Specialist) **Due Date:** Complete

.

Appendix 1

Key issues and recommendations *(continued)*

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
3	❸	**Password Parameters Configuration - SAP** We reviewed the SAP System Screen which records the password parameters (the RSPARAM SAP table). As a result of this we identified that one of the parameters (‘min_password_diff’) was set to “1”. The result of this is that the difference between consecutive passwords would only need to be one character in order for the password to be valid. In our view this is an inadequate degree of change and new passwords may be too similar to the prior password and therefore reduce the security offered. Password parameters are a key element of any system’s security arrangements. Where the parameters are not sufficiently robust there is an increased risk of user accounts becoming compromised and unauthorized access being obtained. **Recommendation** The Authority should amend the system parameter so as to require a higher degree of variation between passwords and force users to define more secure passwords.	SAP password parameters are maintained in accordance with the Corporate Password policy and, as in this case, where specific detail is not in said policy, aligned to the prevailing corporate network password configuration. By implementing this recommendation we would be moving away from alignment to the Council’s approved network password standard. Given that a user must first log on to the network before they can access SAP, we feel that the increase in support overhead and calls to the service desk generated by such a change would significantly outweigh the perceived security benefit. This recommendation will therefore not be implemented. **Responsible Officer:** Stuart Honeyball (Application Support Manager) **Due Date:** N/A - Rejected

.

Appendix 2

Follow-up of prior year recommendations

The Authority has made progress in the implementation of the recommendations raised in our *Interim Audit Report 2013/14.*

We re-iterate the importance of the outstanding recommendations and recommend that these are implemented as a matter of urgency.

This appendix summarises the progress made to implement the recommendations identified in our Interim Audit Report 2013/14 and re-iterates any recommendations still outstanding.

Number of recommendations that were:		
	Non-IT	IT
Included in original report	1	3
Implemented in year or superseded	-	1
Remain outstanding (re-iterated below)	1	2

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
1	2	**Access and Monitoring of high privilege SAP Access** *A number of recommendations have been raised over previous years in relation to SAP access which have now been combined.* CGI provide support to the SAP environment through an agreed contract and consequently have access to the 'Access to all' system privileges for example the SAP_ALL profile. As a result of CGI working practices a large number (approximately 230) of CGI staff could access these key accounts which we consider to be excessive when limited monitoring controls are in place. Direct changes to data via the SAP Graphical User Interface (GUI) is restricted by technical controls to lock the live production environment and enforce changes to be actioned through non-production environments. Monitoring is carried out to ensure that these controls are operating effectively and it was identified that this had identified an occurrence where a change had been inappropriately processed by CGI. There is a risk that unauthorised changes are made to the data in the live system which remain undetected.	This matter was fully discussed with KPMG at the last audit. Wiltshire's approach to this control is in line with industry standards and other local authorities in respect of their ERP systems. Reports and other compensating controls are in place to minimise the risk.	**Remains outstanding but the risk has reduced** Significant improvements have been noted in the controls around SAP privileged access. Access to critical financial transactions and the ability to unlock production are being appropriately monitored. However, two issues remain outstanding: ▪ CGI still hold access to the SAP_ALL profile ▪ Accounts TMSADM and SAPCPIC on a number of non-production environments have well known passwords

Follow-up of prior year recommendations *(continued)*

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
1	2	**Access and Monitoring of high privilege SAP Access** ***(continued)*** **Recommendation** Restrict access to the underlying database to a minimal number of users, particularly where write/amend/delete access is granted. Such access should be appropriately logged and monitored. The Authority should also consider enabling the tracking of changes to the data held within SAP database tables (table logging). Where possible, periodic review of table logs should be implemented to reduce the risk of unauthorised changes.		**(continued)** Our sample testing has also identified that CGI has granted itself the SAP_NEW profile for 36 seconds without following the appropriate process. We recommend that CGI's access is restricted to transactions relevant for providing support and that the aforementioned passwords are changed. **Management response update** **CGI hold SAP_ALL profile** – As in previous audits, this level of access is an agreed, accepted and necessary part of the support arrangements we have in place with CGI. No action required. **System accounts with well-known passwords** – as noted, these accounts were in non-production clients, and the passwords have now been amended.

.

Appendix 2

Follow-up of prior year recommendations *(continued)*

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
1	2	**Access and Monitoring of high privilege SAP Access** ***(continued)***		**(continued)** **SAP_NEW profile added by CGI** – This was added in error for a period of 36 seconds but this did not represent any increase in risk. The concern identified was the addition of the profile without recourse to the correct procedure for requesting such access; this has been reiterated to our CGI account manager for cascading to the relevant teams. **Restrict CGI access to limited transaction** – As agreed in previous audits, this level of access is an agreed, accepted and necessary part of the support arrangements we have in place with CGI. Significant operational difficulties for both the business users and ICT would result in limiting CGI access in as proposed, due to the proactive monitoring and 24x7 response requirements of the support delivered by CGI under our contract with them.

.

Appendix 2

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
2	❸	**Internal audit review** We have identified one improvement point in relation to clearer documentation on working papers of the linkage between expected controls found to be absent, and mitigating controls identified. **Recommendation** SWAP should ensure that the where control deficiencies or absences are identified any mitigating controls are appropriately tested and documented.	Agreed and in progress **Responsible Officer:** Michael Hudson (Associate Director, Finance and Pension Fund Treasurer) and David Hill (Director of Planning, SWAP) **Due Date:** September 2014	**Remains outstanding** Although there has been increased effort to document linkage between controls and mitigating controls it still is not evident through all of the work that we reviewed. Specifically in payroll where the mitigating control over missing starter forms was not clearly documented in the work, we were only able to note it through discussions with internal audit. **Management response update** David Hill (Director of Planning, SWAP) has reviewed this and accepted that there is room for improvement and will therefore be delivering further training for all staff on this.

Appendix 2

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
3	❸	**Removal of user access - Civica** Leavers cannot be clearly identified on the Civica WebPay system as a result of limited information within the system and the fact that the Syntax for the userID does not allow for the full user name. The Civica Workstation system does not permit the disablement or deletion of user accounts. Passwords are reset when the system administrator is notified that a user has left, however, there is no mechanism whereby this can be verified. The system administrator also confirmed that regular reviews of users are not carried out to ascertain if all system users are current and the level of access appropriate for their role. By not removing user accounts for users who have left, there is a risk that access to Authority data could be gained by unauthorised persons. **Recommendation** Due to the system limitation it is more vital that regular reviews of users are carried out to identify where users have left or have changed roles and no longer require their current level of access.	Procedures have now been put in place whereby the Civica System Administrators receive monthly updates on starters, leavers and movers from the HR system. This list is used to revoke / update access to the system. A full review post audit has now been carried out and open accounts where staff known to have left have been disabled. **Responsible officer:** Neil Salisbury **Date:** 1 December 2012	**Remains outstanding** Despite improvements to the process, our testing of 100% of leavers have identified nine Webpay accounts that had been disabled between 10 and 89 days after the users' leaving dates. It was confirmed that none of these accounts had accessed the system after the users' leaving date. **Management response update** The Civica administrators receive a weekly report of starters, leavers and role changes. Therefore, a delay of up 7 days may have already occurred. This report is actioned swiftly, but a small additional delay may elapse before an account is disabled. The system will automatically disable any account that is inactive for a period of 90 days. Also, a valid Wiltshire network login is required to access the system.

Appendix 2

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2015
3	❸	**Removal of user access - Civica** **(continued)**		**(Continued)** A small number of these delays fall outside of our expected timescale however the compensating controls mentioned mitigate the already small risk involved. This process will be reviewed to try and capture all required disablements within expected timescales

KPMG

cutting through complexity™