KPMG

cutting through complexity™

Interim Audit Report 2011/12

Wiltshire Council

June 2012

Contents

The contacts at KPMG in connection with this report are:

Chris Wilson
Partner
KPMG LLP (UK)

Tel: 0118 964 2269
christopher.wilson@kpmg.co.uk

Darren Gilbert
Senior Manager
KPMG LLP (UK)

Tel: 02920 468205
darren.gilbert@kpmg.co.uk

Rachael Tonkin
Manager
KPMG LLP (UK)

Tel: 0117 905 4654
rachael.tonkin@kpmg.co.uk

Duncan Laird
Assistant Manager
KPMG LLP (UK)

Tel: 0117 905 4253
duncan.laird@kpmg.co.uk

Introduction

This document summarises the key findings arising from our work to date in relation to both the audit of the Council's 2011/12 financial statements and the 2011/12 VFM conclusion.

Scope of this report

This report summarises the key findings arising from:

- our interim audit work at Wiltshire Council (the Council) in relation to the 2011/12 financial statements; and
- our work to support our 2011/12 value for money (VFM) conclusion up to June 2012.

Financial statements

Our *Financial Statements Audit Plan 2011/12*, presented to you in March 2012, set out the four stages of our financial statements audit process.

During March 2012 we completed our planning and control evaluation work. This covered our:

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

VFM

Our *External Audit Plan 2011/12* explained our risk-based approach to VFM work, which follows guidance provided by the Audit Commission. We have completed some early work to support our 2011/12 VFM conclusion. This included:

- assessing the potential VFM risks and identifying the residual audit risks for our VFM conclusion;
- considering the results of any relevant work by the Council, the Audit Commission, other inspectorates and review agencies in relation to these risk areas; and
- identifying what additional risk-based work we will need to complete.

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 2011/12 financial statements and VFM.

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. Last year we were unable to rely upon the IT control environment. Improvements have been noted within the control environment in relation to control of powerful user access, user administration and logging of program changes. However, controls implemented during the financial year remain immature and further enhancements could be made which we have recommended. As a result of the quality of the IT controls, significant weaknesses in the control environment remain. Further recommendations have been identified this year, which if implemented should enable the SAP environment to be deemed 'effective' from an audit viewpoint. As a result of our findings on user access and program changes, we are again unable to rely fully on your IT control environment. We note, however, the positive direction of travel that the Council has achieved in addressing last year's recommendations. It is also important to note that the issues identified do not mean there have been fundamental failings in the day to day operation of the Council's IT systems. Rather that the weaknesses we have continued to find mean we cannot rely on the operation of certain key controls to gain the assurance that we require for our audit.
Controls over key financial systems	The controls over the majority of the key financial system are generally sound. However, there are some weaknesses in respect of individual controls in respect of the Revenue & Benefit systems which means we will need to complete additional substantive work at year-end on the year reconciliations and data transfer. At the current time, it is hoped that the additional work will not create additional costs as we plan that the work will be absorbed into the year end audit. However, this is dependent on how the year end audit progresses and will need to be reviewed at the end of the final audit visit.
Review of internal audit	The Council's internal audit function was outsourced to the South West Audit Partnership (SWAP) part way through the year. This change inevitably had an impact on internal audit during the year, but despite this we found that Internal audit generally complied with the *Code of Practice for Internal Audit in Local Government*. We were able to place reliance on some of internal audit's work on the key financial systems. We were able to place partial reliance on internal audit's IT audit work but we had to extend the level of testing in several cases. We are now holding quarterly meetings with SWAP to ensure we develop a closer working relationship.
Accounts production and specific risk areas	The Council's overall process for the preparation of the financial statements is sound. The Council 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.
VFM audit	Our VFM audit risk assessment and work to date has provided good assurance on the Council's arrangements to secure value for money on its use of resources. We have completed this initial risk assessment and consider that the Savings plan is the key risk for the Council at present. We have also completed a series of interviews with the Corporate directors to support our VFM programme of work. We still have to complete our programme of audit work to inform our value for money conclusion, to be issued in September alongside our opinion on the Council's accounts.

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.

In previous years we used our work on the Use of Resources assessment to inform our findings in these areas. Due to the reduced scope of the VFM assessment we have to complete more specific work to support our financial statements opinion.

We obtain an understanding of the Council'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 assessment for 'information systems relevant to financial reporting' reflects the findings from our review of your IT control environment.

The grading has been assessed as a '2' as a result of the IT control environment findings (on the next page) and that we are aware that the Finance team do complete a significant level of extra work to provide assurance on the financials, which is inefficient. We are aware of a SAP implementation programme is being completed at present on the end user SAP reporting environment.

Aspect	2011/12 Assessment	2010/11 Assessment
Organisational structure	3	3
Integrity and ethical values	3	3
Philosophy and operating style	3	3
Participation of those charged with governance	3	3
Human resource policies and practices	3	3
Risk assessment process	3	3
Information systems relevant to financial reporting	2	2
Communication	3	3
Monitoring	3	3

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

IT control environment

Our review of your IT control environment is confirm that improvements have been made from last year. However, we are again unable to fully rely on the Council's general IT control environment.

Work completed

The Council 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, system development and computer operations.

In completing this work, we can partially rely on internal audit's reviews of SAP (general ledger), Northgate (Revenue & Benefits) and Civica Icon (cash receipting). This has been complemented by our own testing of the controls over:

- physical and logical access to the Council's IT systems and data;
- system changes and maintenance;
- the development of new systems and applications;
- computer operations, including the processing and backup procedures; and
- the monitoring and accuracy of end-user computing.

In relation to Simdell (Housing rents) and overall network controls we have reviewed internal audit's findings and found these to broadly mirror our findings from last year. Given that Simdell is scheduled for replacement this year, and taking into account our findings in relation to SAP, Northgate and Civica, we have not carried out any further work in these two areas.

During the course of the year the Council implemented a new version of the Northgate Revenue and Benefits system, which combines data from all of the previous councils' legacy systems. A review of the controls over the transfer of data in relation to this system is being completed by internal audit, and will be reviewed and supplemented by KPMG, as a distinct piece of work our related findings will be reported separately in our ISA 260 report in September. The timetable for this separate assurance work has unfortunately been delayed. We anticipate that the work will be completed in the next few weeks in time for the final audit visit in July.

Key Findings

Aspect	2011/12 Assessment	2010/11 Assessment
Access to systems and data	1	2
System changes and maintenance	1	1
Development of new systems and applications	2	N/A
Computer operations, incl. processing and backup	3	2
End-user computing	3	N/A

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

We again note that further improvements have been made, in the current year, in respect of the IT control environment, particularly in relation to the SAP system.

However, the control environment remains immature following the recent major SAP implementation programme and also the in-sourcing of the IT function from Steria. Our assessment of 'Access to Systems and Data' is Category 1. This is due to the high number of control deficiencies across all the key financial systems and the issues remaining over the control of powerful users accounts from prior year recommendations. It is now critical that these weaknesses are fully addressed to enable the IT control environment to strengthen overall and to be able to progress to the next level.

IT control environment (continued)

Our assessment of 'System Changes and Maintenance' is also Category 1, owing to the high number of SAP generic user accounts which enable access to the underlying SQL database which holds all SAP data, which weakens any segregation of duties controls.

Due to the issues identified above we found your IT control environment is ineffective overall for our audit purposes. We noted a number of areas for further improvement.

The following three points explain the key issues identified during the 2011/12 IT audit:

- **Protection of the SAP production environment from direct changes –** There are still a significant number of SAP generic user accounts held by Logica support staff. There is also a lack of compensating monitoring controls in place to ensure that direct database access is appropriate. Although, there are detailed contractual obligations in place between the two parties, from an audit point of view there are no adequate controls to gain comfort that this level of access has not been used inappropriately by an individual user e.g. to bypass operational segregation of duties controls, to directly change underlying data or to make unrecorded changes to the SAP production environment. **(Recommendation 2)**
- **Powerful user accounts** - In respect of the Northgate ICON system there are no formal monitoring procedures in place surrounding Council staff and third party remote application support providers who have powerful access rights within the live environments. Therefore, the same potential concerns as noted above for the similar SAP issue also apply to this system. **(Recommendation 6,10 and 12)**
- **Access to Sensitive SAP transactions –** Control failures have been identified around user administration procedures, in particular against timely removal of user access for staff leavers. In addition, there is a lack of a formalised and complete regular user access review process across all key financial systems. This means that we gain less assurance that appropriate segregation of duties within an application has been maintained throughout the financial year. **(Recommendation 4)**

It should be noted that the issues identified do not mean there have been fundamental failings in the day to day operation of the Council's IT systems. Rather that the weaknesses we have continued to find mean we cannot rely on the operation of certain key controls to gain the assurance we require for our audit.

We will alter our audit strategy to take account of these findings when completing the substantive testing during our final audit visit in July. This will involve direct extractions being made from underlying data for analysis and therefore avoiding placing reliance on key automated controls within SAP.

Recommendations are included in Appendix 1.

Controls over key financial systems

The controls over the majority of the key financial system are generally sound.

However, there are some weaknesses in respect of:

- **timely completion of reconciliations of the Council tax and Housing Benefit systems following the transition to the new Northgate system.; and**
- **evidence of completion of bank reconciliations.**

Work completed

We work with your internal auditors to update our understanding of the Council's key financial processes where these are relevant to our final accounts audit. We confirm our understanding by completing walkthroughs for these systems.

We then 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 key 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.

This year our audit approach has been amended so that we have not defined payroll, non payroll expenditure, treasury management and benefits expenditure as systems requiring detailed controls testing, as a result of the low risk of material misstatement occurring. This assessment is on the basis that there is a high volume of low value transactions, with a low level of complexity and with a low level of judgement involved in the transactions, as well as good coverage by internal audit. In addition to that the audit last year, both at the interim and final did not identify any material errors or weaknesses in the systems. In addition, we complete detailed testing on the benefits expenditure during the Housing Benefit count audit in August, so we will utilise these findings and not duplicate audit effort during the interim audit visit.

Detailed audit work will be completed during the final audit visit which will focus on substantive analytical procedures. If issues are identified with these tests then further work will be completed but based on our current risk assessment, we are not expecting any material misstatements.

Key findings

The controls over the majority of the key financial system are generally sound but we noted some weaknesses in respect of individual financial systems.

- Cash - Lack of evidence of review of bank reconciliation; and
- Council tax and business rates - Lack of timely completion of reconciliations completed following the transition to the new Revenue & Benefits system (Northgate).

We have made one recommendation for Cash which in appendix 1.

Recommendations for Council tax and business rates have already been made by internal audit on the weaknesses identified and therefore we are not repeating then in this report.

Our plan for the final audit visit is that we will audit the year end bank reconciliations and we will also audit the year end reconciliations of Council tax and housing benefit.

We have not yet assessed the controls over financial reporting as this area is mainly operated during the closedown process and our testing will be supplemented by further work during our final accounts visit.

System	Assessment
Housing rents income	3
Council tax income	2
Business rates income	2
Cash	2
Asset management	3
Financial reporting	TBC

Key:
1 Significant gaps in the control environment.
2 Deficiencies in respect of individual controls.
3 Generally sound control environment.
TBC To be tested during the year end audit

Review of internal audit

Internal audit generally complies with the *Code of Practice for Internal Audit in Local Government.*

This has been a difficult year for internal audit with a significant level of change leading up to and after the introduction of SWAP as the Council's internal audit provider.

The Council now needs to fully engage with SWAP, as their internal auditors, rather than treating them as an outsourced provider.

Work completed

We work with your internal auditors to assess the control framework for 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 Council'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 Code of Practice for Internal Audit in Local Government (the Code) defines the way in which the internal audit service should undertake its functions. We assessed internal audit against the eleven standards set out in the Code.

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

Key findings

Following a review of the work of internal audit work we have been able to place partial reliance on their work. In the case of IT audit we completed additional testing as detailed in page 5.

We have completed the assessment of internal audit based on review of their working papers and our knowledge through our work during 2011/12.

Based on our assessment, internal audit generally complies with the Code.

There have been significant changes in the delivery of the internal audit during the year and so it has been a year of transition. Internal audit commenced the year as an in-house team, however the Head of Internal Audit left in May 2011. During the intervening period the three principle auditors jointed acted as the HIA until the start of November. At the start of November, the internal audit service was outsourced to South West Audit Partnership (SWAP) and the staff were transferred to SWAP.

The internal audit team has had to work through this difficult period of change.

Internal audit took the decision not to adopt the SWAP computerised working papers at the time of transfer and retained their previous audit approach and working practices for the remaining audits in the 2011/12 audit plan. However, the new processes have now been adopted for the 2012/13 year. As a result of this decision, the working practices and approach of internal audit did not significantly alter in 2011/12.

Aspect	2011/12 Assessment	2010/11 Assessment
Scope of internal audit	3	3
Independence	3	3
Ethics for internal auditors	3	3
Audit Committee	3	3
Relationships with management, other auditors and other review bodies	3	3
Staffing, training and development	3	3
Audit strategy and planning	3	3
Undertaking audit work – Non IT audit	2	2
Undertaking audit work – IT audit	1	1
Audit strategy and planning	3	3
Due professional care	3	3
Reporting	3	3

Key: 1 Significant areas for improvement
2 Areas for improvement.
3 Satisfactory

Review of internal audit (continued)

Key findings

In the table on the previous page, we have split the assessment of 'Undertaking audit work' into two sections being IT and Non IT work. We have maintained the grading as per the prior year's assessment with non IT work as a '2' as a result of some deficiencies with the documentation of the testing.

The IT work has been graded a '1' as a result of the continued weaknesses in the quality of the audit work. The internal audit findings were mainly consistent with KPMG's findings and conclusions. However, the approach taken by internal audit was not complete and KPMG had to complete additional testing to gain the level of assurance required. The details of these weaknesses have been discussed with SWAP. In addition internal audit did not clearly test both the design and implementation of a control together with the operating effectiveness. The documentation of internal audit findings could also be improved as this remained on Wiltshire Council's previous approach.

In addition, following the change to SWAP we understand that the internal audit team have experienced systems access issues, which has led to significant delays in the audit timetable. This has particularly impacted on the IT audits and the internal audit work of the Revenue & Benefits data migration testing.

These issues have been discussed with SWAP and we anticipate that they will be addressed by Wiltshire Council resolving the access issues of the SWAP members and with SWAP introducing their electronic working papers together with providing a more consistent resource within the IT audit function.

We recommend that we complete a full review of the internal audit function in 2012/13 when SWAP has been fully embedded.

We have retained the recommendations for improvement identified in 2010/11 audit, rather than generating new recommendations, as we consider that the two recommendations cover the weaknesses identified in internal audit in the current year. A status update of the 2010/11 recommendations is provided in Appendix 2.

Looking forward, we are developing a positive and productive working relationship with SWAP and have already held planning discussions aimed at supporting and improving our ability to rely on internal audit's work next year. We look forward to developing this relationship further.

Accounts production process

The Council's overall process for the preparation of the financial statements is adequate.

Work completed

We issued our Accounts Audit Protocol to Finance on 30 March 2012. This important document sets out our audit approach and timetable. It also summarises the working papers and other evidence we require the Council to provide to support our audit work.

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

As part of our interim work we specifically reviewed the Council's progress in addressing the recommendations in our *ISA 260 Report 2010/11*.

Key findings

We consider that the overall process for the preparation of your financial statements is strong.

There were no high level recommendations issued during the 2010/11 audit.

Last year the Council managed the year end close down process very well and we do not anticipate any change to it this year.

However, this year the final sign off timetable has been tightened, so that it is planned that the financial statements will be signed at the Audit Committee meeting on the 7 September, rather than at the end of September which has always been the case in prior years.

The start of the audit has not yet moved forward, so the finance team has the same length of time to prepare for the audit as last year. However, the change of the final signing does require that all issues raised during the audit are cleared on a timely basis.

At the current time, we are confident that both the Wiltshire Council finance team and the KPMG audit team will be able to meet the new timetable.

Specific risk areas and VFM

The Council 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.

Work completed

In our External *Audit Plan 2011/12*, presented to you in March 2012, we identified the key risks affecting the Council's 2011/12 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 the finance team as part of our meetings. In addition, we sought to review relevant workings and evidence and agree the accounting treatment as part of our interim work.

Key findings

The key risks identified in the plan included:

- public Sector cuts and the council's saving plans;
- code change which includes the requirement to account for heritage assets;
- revenue and benefit system changes; and
- estate property changes.

These risks were considered during the interim audit visit and will be the focus of work during the year end audit visit in July to ensure that the risks are monitored and addressed throughout the audit process and our findings will be reported to you in September.

There were two further risks identified in the plan where audit work has already been completed and the findings have been reported to you within this interim report.

- SAP operating effectiveness (see pages 5 and 6); and
- Internal audit (see pages 8 and 9).

VFM audit approach

Our VFM audit risk assessment and work to date has provided good assurance on the Council's arrangements to secure value for money on its use of resources. We have completed this initial risk assessment and consider that the savings plan is the key risk for the Council at present and will consider this further during our final audit.

We still have to complete our programme of audit work to inform our value for money conclusion, to be issued in September alongside our opinion on the Council's accounts.

Key issues and recommendations

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

The Council 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		
1 ***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.	2 ***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.	3 ***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	2	**Evidence of review of bank reconciliation** The bank reconciliations are prepared in excel monthly, and are reviewed on screen. As a result there is no evidence that the control is being carried out. As the review is being completed on screen no audit trail exists. There is no evidence that the reconciliation has been independently reviewed by a more senior member of the team which could potential identify errors. The lack of audit trail, also means that it is not possible for the auditors to check to review process is completed on a timely basis. We acknowledge that the finance team want to keep records electronically and do not want to resort to printing out the reconciliation and signing it. However, we recommend that the excel document is signed off electronically and saved on the system for evidence of review. We suggest that the Finance team investigate electronic sign offs as it is possible for a signature to be attached to an individual by their log in and therefore is not just typing their name.	Wiltshire Council has in place a fully automated bank reconciliation process. This is undertaken on a daily basis and is regularly reviewed by management. This includes periodic reconciliations completed by the manager. The reviewer will e-mail confirmation to the Chief Accountant on a regular basis that the reconciliation has been reviewed to strengthen the audit trail. Responsible officer: Stuart Donnelly/Matthew Tiller Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
2	1	**Protection of the production environment from direct changes - *SAP*** The underlying SQL database that holds all SAP data can be accessed using generic user accounts by up to 237 Logica staff. This is considered to be a high volume of users. There is also a lack of compensating monitoring controls in place to ensure that direct database access is appropriate. 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. However, no monitoring is carried out to ensure that these controls are operating effectively and that the production environment and the production client has remained locked from direct changes. There is a risk that unathorised changes are made to the data in the live system which remain undetected. **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 Council 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.	A mitigating control has been discussed with KPMG, which management will discuss with the Logica service delivery team. This control is whether Logica have a current ISAE3402 report which will provide assurance to KPMG of Logica's control environment. Responsible officer: Stuart Honeyball Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
3	2	**Standard SAP super user accounts** Standard SAP super user accounts are not appropriately controlled in all instances of SAP. Such accounts are generic and possess the powerful SAP_ALL profile, allowing access to all system functionality. Accounts should be maintained in a locked state with complex passwords and used only where necessary. In such a case, use of the account should be appropriately requested, approved, monitored and documented. It was noted that the greatest risk lies in the unlocked account (DDIC) in the production client. This was stated to be necessary in order for system jobs to execute. **Recommendation** SAP standard user accounts should be locked in all clients and passwords made non-trivial. Dependencies on SAP standard user accounts should be removed where possible and replaced by system or communication type accounts that cannot be accessed by end-users.	The SAP support team have reviewed and continue to review on a monthly basis, the standard transactional activities used across the business and amend as required. Responsible officer: Stuart Honeyball Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
4	2	**Access to sensitive SAP transactions** A number of users were noted to possess access to sensitive SAP transactions that were not required according to their job role and requirements. It was noted that user access to the above transactions is in some circumstances validated by business requirements. **Recommendation** Access to sensitive SAP transactions should be reviewed to ensure that access is restricted to only those users that require the functionality according to their job role and requirements. Where business reasons exists for access to such transactions, this should be appropriately documented, approved and monitored. Enforce segregation of duties for IT and business users with any known exceptions subject to further documentation and appropriate approval.	Many of these transactions cover standard transactions and have been reviewed and amended. An ongoing monthly review process is in place. The SAP team continue to produce documentation to cover sensitive transactions and any changes made to them to ensure they are properly controlled, recorded and maintained. Responsible officer: Stuart Honeyball Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
5	3	**Resolution of problems directly in the SAP production environment** A small number of instances were identified during the financial year where testing for problem resolution was carried out directly in the live production environment. It was stated that taking action in the production environment only occurred where alternative actions had already been carried out. Despite this, there is a risk that the production environment may be negatively impacted by performing un-tested problem resolution activities. **Recommendation** Resolution of problems directly in the production environment should be avoided wherever possible. Such activities should be carried out in a non-production environment that appropriately mirrors the production environment to validate testing performed. This will ensure that there is no risk to the integrity of the production environment whilst performing problem resolution activities.	The auditors recommendations are noted. The Council's standard approach to applying problem fixes is through the development and test systems for testing before release into production. Only in exceptional circumstances are fixes applied directly to live, and then such releases are tightly managed. The system is backed up enabling a restoration to previous state if necessary. Responsible officer: Stuart Honeyball Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
6	1	**Powerful User Accounts - *Northgate*** There are a number of generic powerful user accounts in use for the Northgate system. Although an audit log is produced of all action carried out using these accounts, they are not reviewed and are overwritten every 4 weeks. This may result in the inability to attribute actions to an individual user or unauthorised persons gaining access to the system data. **Recommendation** The use of generic powerful user accounts, where more than one member of staff has access, should be kept to a minimum. Where they are required, regular monitoring of who has access to them should be carried out and a random sample of audit logs reviewed by a senior independent manager.	Access details for the powerful user accounts within the Northgate system are restricted to the Revenues and Benefits system team members. These team members have user accounts with the same level of access as these powerful users in order to minimise the circumstances when these accounts need to be used. The recommendation that the use of these accounts is monitored is accepted and procedures will be put in place for the Systems Manager and Head of Revenues and Benefits to do so on a four weekly basis. Responsible officer: Sally Kimber/Ian Brown Date: 1 July 2012
7	2	**Removal of user access - *Northgate*** The appropriate line manager is required to complete a leavers form for all leavers which is either emailed or sent in hard copy to the System Administrator, who will then revoke the user's access to Northgate. However, it was noted that very few leavers forms are received by the System Administrator If the System Administrator is not notified of all leavers in a timely fashion there is a risk that unuathorised persons may have access to the system data. **Recommendation** Remind all line managers of the requirement to promptly notify the System Administrator of all leavers.	Recommendation is accepted and in addition, the current users of the system will be checked on a regular basis to the Wiltshire Council directory to ensure that if any leavers have been missed, the relevant line manager can be contacted. Responsible officer: Sally Kimber Date: 30 June 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
8	3	**Password Configuration Settings - Northgate** Password complexities within Northgate are managed on a profile basis. Each user is assigned to one of 8 individually configured profiles. Of the 8 profiles identified, 7 were noted to have an adequate level of complexity. The password parameters for the remaining profile, "FIRST_DEFAULT, do not comply with the Council password policy. **Recommendation** Amend the password parameters for the "FIRST_DEFAULT" profile in line with the Council's password policy.	Wiltshire Council has approached Northgate for advice regarding this recommendation as although it is accepted, management need to establish if there are any other implications that should be taken into account as this profile is used by the generic user accounts which are used to run specific jobs/processes. Responsible officer: Sally Kimber Date: 30 June 2012
9	3	**Review of user access - Northgate** No reviews of the appropriateness of user access has been performed since July 2011 and no documentary evidence has been retained for any reviews previously carried out. Without a regular review of system users there is a risk that unauthorised users may have access to the system data. **Recommendation** Undertake a review of all users on a regular (e.g. six monthly) basis to ensure that the level of access remains appropriate and all accounts for users who have left have been removed.	Recommendation accepted. Responsible officer: Sally Kimber Date: 31 July 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
10	2	**Powerful user accounts - *Civica*** Powerful "system Administrator" access to Civica WebPay is controlled via assignment to the administrators user group. However, the System Administrator advised that, due to limitation in the system, it was not possible to generate a list of all users assigned to the administrators user group. "System Administrator" access within Civica Workstation is controlled via assignment of level 20 access. Of the 11 live accounts assigned with level 20 access, two ("system Administrator (001)" and "system Administrator (ww)") were identified for which the System Administrator was not aware of their purpose or who may have access to them. Of the two Civica databases one is hosted by the supplier and one by the Council. Council staff only have direct database access to Workstation. Access to the database is obtained via one of five SQL Database accounts. Of these two were disabled at the time of the audit. Of the remaining three accounts one is used by the application and cannot be used by an individual. Access to the remaining two accounts is restricted to a small number of ICT staff. No review of access is performed and passwords are not subject to periodic change. Without proper controls over such powerful user accounts there is a risk that unauthorised changes to the system data could be made and remain undetected. **Recommendation** The purpose of the two level 20 user accounts in WebPay which the System Administrator is unaware of should be investigated and, if appropriate, deleted. For the two SQL Database accounts , to which ICT staff have access, a log should be maintained showing who had access to the accounts and the date.	At application level, the 001 account is used by automated system jobs and is not assigned to a real user. Will review the requirement and usage of the 001 account and other admin level accounts. There are two separate Civica databases: The WebPay database is hosted by the supplier. Wiltshire council staff have no direct access to this. The local 'workstation' database is stored on Wiltshire systems. Access is controlled by ICT. The 'ICON' account is used in the setup of the application. We will investigate the options around recording who has used the generic accounts on specific dates. Any issues etc are investigated and dealt with on an exceptions basis as all transactions are logged and traceable. Responsible officer: Neil Salisbury Date: December 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
11	2	**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 Council 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.	We will undertake annual reviews of user accounts starting December 2012. Responsible officer: Neil Salisbury Date: 1 December 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
12	2	**Monitoring of powerful user access by third parties - *Civica*** Access by external persons to the WebPay system is gained using the generic Administrator account. This is enabled only as and when requested. The availability of this account is managed exclusively by the System Administrator. Although a call is logged within the Civica support desk a call is not logged with the Council support desk. This is in contravention of the Council's policy. Third party access to the Workstation system is obtained through the use of the Civica_comino domain level user account. In order to access this account Civica are required to contact IT who issue a unique code, generated by a VPN secureID token which will enable Civica to connect to the Council network. The System Administrator confirmed that no monitoring is performed of actions undertaken by external users on either of the above accounts. **Recommendation** A call should be logged with the IT help desk to record when Civica have been granted access to the WebPay system. The System Administrator should carry out a periodic check of any changes made to the Workstation system using the Civica_Comino Domain account.	WebPay is hosted by Civica. They therefore have full access to the system environment. They are contractually obliged to provide a working system. However, they have no 'user' access to the application unless granted by Wiltshire. This is rare and is usually in response to a support call. We will look to get ODBC access (read only) to the hosted database to enable direct enquiries on user activity. We will ensure that a call is logged with Wiltshire's IT Service Desk when 'user' access is granted to Civica support personnel. The Civica_comino domain account is a Windows account. It carries no application access. Therefore, no direct changes can be made to the application using this account. – In order to gain access to the application as a 'user', this would have to be enabled by the system administrator. Responsible officer: Neil Salisbury Date: No further actions proposed.

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
13	3	**Changes to system configuration - *Civica*** The System Administrator advised that configuration changes for Civica workstation such as changes to the processing rules are generally actioned by the system administration team and are. These changes are not logged within the service desk and are not subject to independent approval or progression via the ICT change control process. Changes are done in the test environment prior to being actioned in the live environment. Changes are performed by System Administrators using level 20 access. As these changes are not logged there is a risk that unauthorised changes could be made to the system configuration and impact on the accuracy or the system data. **Recommendation** All configuration changes should be logged with the service desk.	Considered minor risk. Major system changes (new interfaces / upgrades etc) are formally tested and recorded. However, it is neither practical nor preferable to log ALL changes with the service desk and little if anything would be achieved by such procedures. Responsible officer: Neil Salisbury Date: No actions proposed.

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
14	3	**Access to migrate changes to the Civica production environment** Access to migrate data to the test the live environments is performed via a generic SQL Database owner level account (ICON). The System Administrator confirmed that access to this account is restricted to a limited number of ICT personnel. However, the account password is not subject to periodic changed and the account is not monitored to validate or monitor any actions performed. The account password is stored within a central spreadsheet held by the security team. **Recommendation** Undertake a regular independent review of actions carried out using the ICON accounts.	Any issues are investigated on an exceptions basis. The 'ICON' account is used for ALL ODBC connections by the application. Therefore to attempt to conduct a full review of all actions carried out by this account would be unworkable and would achieve little. Responsible officer: Neil Salisbury Date: No further actions proposed.

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
15	3	**Monitoring of scheduled jobs - *Civica*** All jobs are monitored on screen but there are no formal established procedures for conducting daily checks or reporting and resolving any errors caused through the overnight processing. No records of the actions taken to correct errors are maintained. **Recommendation** Introduce a formal process for daily checks on all scheduled jobs, and for reporting and resolution of any errors.	Scheduled jobs are monitored on an exceptions basis. We will implement a log of 'exceptions' to include comments, resolutions etc. Responsible officer: Neil Salisbury Date: 1 December 2012

Key issues and recommendations

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
16	3	**Change Control - *Civica*** All changes to the Civica WebPay are carried out by Civica. Civica will notify the Council of proposed changes and, if the Council does not raise any objections, will action the changes during system downtime. No assurances are received by the Council as to the level of testing carried out prior to the change actioned. For Workstation the System Administrator confirmed that no changes had been made during the financial year. It was noted that there is no documented change control process in place and no documentation is retained of changes made. Without a proper process in place there is a risk that unauthorised or untested changes could be made to the system which may compromise system performance and data. **Recommendation** Document the process for review, development, testing and approval of all system changes to the workstation. When changes are made documentation should be retained to provide evidence that the proper process had been followed.	For WebPay (hosted), Civica are contractually obliged to provide an up to date system. Therefore they apply software patches etc directly. Version / functionality upgrades etc are controlled by Wiltshire and are tested and logged etc. A basic process for upgrades etc will be documented. Responsible officer: Neil Salisbury Date: 1 December 2012

Appendix 2

Follow-up of prior year recommendations

The Council has not implemented all of the recommendations in our *Interim Audit Report 2010/11* and the *ISA 260 report.*

We note that there are several outstanding recommendations from the prior year, but we accept that action has been taken and also events have occurred during the year, which has prevented the Council from fully addressing the recommendation.

We 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 2010/11 and 2010/11 ISA 260 report and re-iterates any recommendations still outstanding.

Number of recommendations that were:		
	Non IT	IT
Included in original report	4	10
Implemented in year	2	-
Remain outstanding, in progress and to be followed up at year end	2	10

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at March 2012
1	1	**Internal audit review of IT controls** We were able to place full reliance on the testing of financial controls and noted improvements in terms of the adequacy of sample sizes used by internal audit. This was not the case for the IT work, where we found that: ■ internal audit's work did not cover all the areas within our agreed joint working protocol and was not documented sufficiently; ■ the work mainly involved only evaluating whether controls were designed appropriately, rather than also testing whether they were effective in practice; and ■ in some cases, the work completed did not support the conclusions drawn. **Recommendation** Internal audit work on IT controls should be performed and documented to the same standards as non-IT audit work.	Principal auditor – IT. Due date: 30 July 2011	**Outstanding** Following the agreement of the recommendation the principal IT auditor did not transfer to SWAP. SWAP have encountered staffing issues within the IT audit team over the year, with several changes in the team and together with the network access issues, has resulted in the recommendation not being addressed. These issues have been discussed with SWAP and these points have been noted and will be addressed. Internal audit will be using SWAP electronic working papers in 2012/13 which will address many of the points including approach and documentation. It has been agreed that the joint working internal/external audit protocol will be revised and re-issued. The main issue from this year's audit was the timing of the work that internal audit was too late and close to the external audit review dates.

Follow-up of prior year recommendations

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at March 2012
1	1	**Internal audit review of IT controls – continued**	Principal auditor – IT. Due date: 30 July 2011	**Management response update - SWAP** Following the transfer of the Internal Audit service to SWAP, the Principal I.T. Auditor, formerly from Wiltshire, did not transfer. This caused some issues in terms of continuity and loss of knowledge in terms of the work that had been undertaken to date. In addition the I.T. Manager from SWAP also left leaving a gap in available I.T. resource. However, whilst some I.T. work was delayed due to staff resources, the main issues were around I.T. infrastructure and network access which are still being resolved at this time. The I.T. audit work undertaken during 2011-12 was a significant improvement in both volume and quality and reports were well received by the relevant Wiltshire Council managers. There are still some areas for improvement and these have been discussed with SWAP and will be addressed during the audit work 2012-13. Internal Audit will also be using MKi, SWAP's electronic working paper systems and audit management tool and this will assist KPMG when they review this work. It has also been agreed that the joint working internal/external protocol will be revised and re-issued to clarify all areas of testing required. Responsible officer: Dave Hill, SWAP Date: 31 July 2012

Follow-up of prior year recommendations

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at March 2012
2	2	**Follow up of control failures by Internal Audit** In a number of cases we found that internal audit had not followed up control failures with additional queries to identify whether there are any compensating arrangements in place, which could then be tested to obtain the assurance necessary. The testing of controls had been performed correctly, but it is also important to respond flexibly if the results are not positive to see if it is possible to achieve the audit objective through an alternative way. **Recommendation** Where control failures are identified by internal audit, they should consider whether there are compensating arrangements in place that may provide assurance on the control objective being tested.	Principal auditors Due date: Ongoing	**In progress** The joint internal/external audit working protocol was re-issued in 2011 to enable internal audit to address these points. As a result of the changes in both governance and also the internal audit team itself through the year, these points have not been fully addressed. However, it has been agreed that a further version of the protocol will be issued in 2012 and that internal audit will now address these issues. It has been agreed that Internal audit will meet with external audit on a quarterly basis to ensure that the teams work more closely together to improve communications and clear any queries or issues on a more timely basis. **Management response update – SWAP** The joint internal/external audit working protocol was re-issued in 2011 to enable internal audit to address these points. However, following a meeting with SWAP in May 2012, KPMG has agreed to further revise and re-issue the protocol to ensure that it is consistent across all KPMG/SWAP clients. It has been agreed that Internal Audit will meet with external audit on a quarterly basis to ensure that both teams work closely together to improve communications and clear any queries e.g. gaps in Internal Audit work, on a more timely basis. Responsible officer: Dave Hill, SWAP Date: 30 September 2012

Appendix 2

Follow-up of prior year recommendations

No.	Risk	Recommendation	Officer responsible and due date	Status as at February 2012
3	1	**Direct changes to live environment – SAP** Introduce immediate logging / alerting of when the SAP production environment needs to be unlocked for direct changes to be made and ensure an adequate audit trail is recorded and retained every time for independent review of appropriateness.	Stuart Honeyball (SAP Support Team Lead)	**In Progress.** See Recommendation 2
4	1	**Monitoring of powerful application user accounts - *SAP*** Continue to identify where powerful user access can be removed if it is not deemed absolutely necessary. Controls should be formally developed to ensure that logs of powerful user access for both Wiltshire Council staff and Logica are sufficient, complete, and reviewed by an appropriately skilled independent resource.	Stuart Honeyball (SAP Support Team Lead)	**In progress**. See Recommendation 2
5a	1	**Change management procedures - *SAP*** Review the access assigned to all users on at least an annual basis to ensure the ongoing appropriateness of user access and ensure formally recorded and appropriately signed-off documentation is retained to support performance of this review.	Stuart Honeyball (SAP Support Team Lead)	**Outstanding**

Appendix 2

Follow-up of prior year recommendations

No.	Risk	Recommendation	Officer responsible and due date	Status as at February 2012
5b	1	**Change management procedures** ***Civica Icon systems, revenues and benefits systems and Simdell*** Ensure Council policies around change management are adhered to with regards to recording / retention of documentation produced for each key stage in the change management process and also for the default disabling of network user accounts used by third party support providers for remote access.		**Civica - Outstanding.** See Recommendation 16 **Simdell** – to be followed up during year end audit **Revenues and benefits** – **Superseded**
6	1	**Use of shared accounts for application administration duties** ***Civica Icon systems, revenues and benefits systems and Simdell*** Review all current user accounts with system administrator privileges for appropriateness of ongoing use. Create separate assigned powerful user accounts between the system administrator and the third party support provider. Also, introduce a regular independent monitoring process over these powerful user accounts (especially those used by the third party support provider).		**Revenues and Benefits - Superseded** **Civica and Simdell** - To be followed up during year end audit

Appendix 2

Follow-up of prior year recommendations

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at February 2012
7	1	**Use of shared accounts for database administration duties** ***Revenues and benefits systems, Civica Icon Workstation*** See comment made against issue number four, and in particular for Northgate consider immediate review and reduction in the number of excess accounts, especially in the development stage of the new Northgate system in December.		**Revenues and benefits - superseded** **Civica - Implemented**
8	1	**Domain / server administrator access - *Network*** Ensure continuance of the internal review and update procedures noted above, ideally to be completed as soon as possible and reduce the number of domain and server level administrator accounts to appropriate and acceptable levels.		**Outstanding**. See Internal Audit Report March 2012, recommendation 7
9a	2	**User access reviews - *SAP*** Review the access assigned to all users on at least an annual basis to ensure the ongoing appropriateness of user access and ensure formally recorded and appropriately signed-off documentation is retained to support performance of this review.	Stuart Honeyball (SAP Support Team Lead)	**Outstanding** It is further recommended that the newly convened SAP System Owners Board are engaged to facilitate such a review, as appropriate engagement from the business is essential to ensure appropriate knowledge of the access required by users is applied to reviews.

Appendix 2

Follow-up of prior year recommendations

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at February 2012
9b	2	**User access reviews - *Network*** Ensure continuance of the overall network user access review process, with particular focus on the more powerful user accounts.		**Outstanding**. See Internal Audit Report March 2012, recommendation 4
10a	2	**Removal of user access for staff leavers – *SAP, Network*** Review the current access removal process to identify where potential improvements could be made to revoke access in a timely manner for user accounts relating to staff leavers and changes in staff position/role.	SAP Stuart Honeyball (SAP Support Team Lead)	**In progress**
10b	2	**Removal of user access for staff leavers** ***Revenues and benefits systems, Simdell*** For Simdell and the revenues and benefits systems, amend the leavers notification process to at least include a regular check (e.g. monthly) of a HR-sourced leavers listing against a full user account listing. For Civica Icon (Webpay), undertake a full review of all current user accounts to identify those that are no longer required and adequately rename the remainder to facilitate a more robust access removal process.		**Civica & Northgate Outstanding.** See recommendation 7 &11 **Simdell – Outstanding.** See Internal Audit report May 2012, recommendation 2

Appendix 2

Follow-up of prior year recommendations

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at February 2012
11	2	**Automated job schedule controls – *SAP*** Ensure that system access to control key jobs / interfaces is regularly checked and introduce a procedure to formally record when key jobs / interfaces are monitored for successful completion.	Stuart Honeyball (SAP Support Team Lead)	**In progress**
12	2	**Access assigned to new/existing users** ***Revenues and benefits systems, Civica Icon Workstation, Simdell*** For the revenues and benefits systems, this procedure should be considered during the systems development stage of the new revenues and benefits system. For Civica Icon Workstation, review current process around new user account creation and ensure approval documentation is retained for at least 12 months to maintain a full audit trail. For Simdell, retain the user access requests and approval communications for at least twelve months before disposal to ensure a full audit trail is maintained.		**Revenues & benefits – Superseded** **Civica - Outstanding. See recommendations 11** **Simdell –** To be followed up during year end audit