



cutting through complexity™

Interim Audit Report 2012/13

Wiltshire Council

May 2013



The contacts at KPMG in connection with this report are:

Chris Wilson

Partner

KPMG LLP (UK)

Tel: 0118 964 2238

christopher.wilson@kpmg.co.uk

Tara Westcott

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

■ Introduction	2
■ Headlines	3
■ Financial statements	5

Appendices

1. Key issues and recommendations	13
2. Follow-up of prior year recommendations	15

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 has issued a document entitled *Statement of Responsibilities of Auditors and Audited Bodies*. This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. We draw your attention to this document which is available on the Audit Commission's website at www.auditcommission.gov.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.

If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Chris Wilson, the appointed engagement lead to the Authority, who will try to resolve your complaint. If you are dissatisfied with your response please contact Trevor Rees on 0161 246 4000, or by email to trevor.rees@kpmg.co.uk, who is the national contact partner for all of KPMG's work with the Audit Commission. After this, if you are still dissatisfied with how your complaint has been handled you can access the Audit Commission's complaints procedure. Put your complaint in writing to the Complaints Unit Manager, Audit Commission, Westward House, Lime Kiln Close, Stoke Gifford, Bristol, BS34 8SR or by email to complaints@audit-commission.gov.uk. Their telephone number is 0844 798 3131, textphone (minicom) 020 7630 0421.

This document summarises the key findings arising from our work to date in relation to both the audit of the Authority's 2012/13 financial statements and the 2012/13 VFM conclusion.

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 2012/13 financial statements; and
- our work to support our 2012/13 value for money (VFM) conclusion up to April 2013.

Financial statements

Our *External Audit Plan 2012/13*, presented to you in March 2013, set out the four stages of our financial statements audit process.



During January to April 2013 we completed our planning and control evaluation work. This covered our:

- 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 with the help of internal audit;
- 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 2012/13* 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 2012/13 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 Authority, 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 and VFM conclusion in relation to the 2012/13 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.

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

Organisational and IT control environment	<p>Your organisational control environment is effective overall.</p> <p>Last year we were unable to fully rely upon the Authority's IT control environment. Improvements have been made within the control environment in relation to control/monitoring of powerful user access (SAP and Northgate) and user administration (Northgate) during the year. However there remains a number of significant prior year recommendations which have not fully been addressed and implemented during 2012/13.</p> <p>As a result of our findings over powerful user access and program changes, we are again unable to rely fully on your IT control environment. We note, however, the continual positive direction of travel that the Authority has achieved in addressing some of 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 Authority's IT systems. Rather, the weaknesses we have continued to find mean we cannot rely on the operation of certain key automated controls to gain the assurance we require for our planned audit approach.</p>
Controls over key financial systems	<p>The controls over the majority of the key financial system are generally sound.</p> <p>However, there are some weaknesses of individual controls in respect of the authorisation and review of journals and the adequacy of documentation relating to reconciliations between Northgate and Civica, and between Northgate and the VOA Reports. These points have already been raised and reported to you by your internal auditors during the year. We will perform increased substantive testing surrounding journals and review the year end reconciliations at our final audit visit.</p>
Review of internal audit	<p>During 2011-12, the Authority outsourced its internal audit function to the South West Audit Partnership ("SWAP"). This inevitably impacted upon the way in which the internal audit function was delivered. During the year we have met regularly with SWAP in order to develop a closer working relationship and to build on our joint working protocol.</p> <p>We have seen a significant improvement on the standard of work produced by internal audit and the increased quality of documentation. We were able to place reliance on internal audit's work in relation to the key financial systems work and the Authority's IT systems. Despite this, there are a few areas where we had to extend the level of testing which mainly related to the size and selection of samples selected by internal audit. Full details are set out page 8.</p> <p>We have undertaken a comprehensive review of SWAP as part of our 2012-13 work, the results of which are being reported separately. Overall, however, we found that Internal Audit generally complied with the Code of Practice for Internal Audit in Local Government.</p>
Accounts production and specific risk areas	<p>The Authority's overall process for the preparation of the financial statements is strong.</p> <p>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.</p>

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

VFM risks

Our VFM audit risk assessment and work to date has provided good assurance on the Authority's arrangements to secure value for money on its use of resources. We have completed this initial risk assessment and consider that the delivery of ongoing savings plans remains the key risk for the Authority at present.

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.

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 in relation to each of the Authority's key IT systems.

Whilst we identified that progress had been made in relation to the adequacy of IT controls compared to last year, further improvements are still required. Further details are provided on the following page.

Aspect	2012/13 Assessment	2011/12 Assessment
<i>Organisational controls:</i>		
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.

Our review of your IT control environment confirms that improvements have been made from last year.

However, we are again unable to fully rely on the Authority's general IT control environment.

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, 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), Simdell (housing rents) and Civica Icon (cash receipting). This has been complemented where deemed necessary by our own testing of the general IT 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; and
- computer operations, including job processing.

During the course of the year the Authority replaced the Simdell housing rents system with a new system called QL. A review of the controls over the transfer of data in relation to this system has recently been completed by internal audit, and will be reviewed and supplemented by KPMG.

This will be a distinct piece of work and our findings will be reported separately. 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	2012/13 Assessment	2011/12 Assessment
Access to systems and data	1	1
System changes and maintenance	1	1
Development of new systems and applications	TBC	2
Computer operations	3	3

- 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, principally in relation to SAP and Northgate systems.

However, our assessment of 'Access to systems and data' overall remains as Category 1. This is due to the high number of control deficiencies across the majority of key financial systems in general and the issues remaining over the control of powerful users accounts from prior year recommendations.

It remains critical that these weaknesses are fully addressed to enable the IT control environment to strengthen overall and to be able to continue to progress to the next level.

Our review of your IT control environment confirms that improvements have been made from last year.

However, we are again unable to fully rely on the Council's general IT control environment.

Our assessment of 'System changes and maintenance' is also Category 1, with key factors being the continued high number of Logica user accounts which enable direct unmonitored access to the underlying SQL database which holds all SAP data (which weakens any related segregation of duties controls).

Due to the issues identified, we found your IT control environment is ineffective overall for our audit purposes.

The following four points explain the key issues identified during the 2012/13 IT audit:

- **Protection of the SAP production environment from direct changes** – Although monitoring of shared powerful user IDs used by Logica support staff at the application level is now fully implemented, the process is relatively basic and there is still a lack of compensating monitoring controls in place to ensure that direct database access is also 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 directly to the SAP production environment.

Also, although Logica are subject to regular (usually six-monthly) independent auditing of their ISO27001 certification, the nature of testing performed looks at the test of design and implementation of controls but does not test the operating effectiveness. This type of certificate is not an adequate alternative to ISAE3402 (or similar) over Logica's IT control environment for the purpose of external audit reliance. (See Appendix 2).

- **Changes made to non-SAP systems** – It was not possible to fully test the effectiveness of the change management process for Civica Icon and Northgate, principally due to lack of formal documentation available and not being able to adequately identify a full list of changes that had occurred through the year. (See Appendix 1).

- **Powerful user accounts** – In respect of the Civica ICON, Simdell and Northgate systems, apart from a new weekly review of one shared powerful user account as used by the third party support vendor for the Northgate application, there are no other formal monitoring procedures in place surrounding user accounts allocated powerful access rights within the live environments at both the database and application levels. Therefore, the same potential concerns as noted above for the similar SAP issue also apply to these systems. (See Appendix 2).
- **Review of user access rights** – Although a robust procedure is now in place concerning Northgate (following a recommendation raised last year), there is still no formal regular process in place for SAP, Civica Icon or Simdell (now defunct). There was an attempt to perform a full user access review in current financial year. However the Authority did not complete this process fully and we are unable to provide assurance on the work performed. (See Appendix 2).

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, due 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.

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

We were able to place reliance on their work.

Work completed

The scope of the work of your internal auditors and their findings inform 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 Code of Practice for Internal Audit in Local Government defines the way in which the internal audit service should undertake its functions. We are currently undertaking a detailed assessment of SWAP against the eleven standards set out in the code. Our findings of this review will be reported separately to you.

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, internal audit are compliant with the *Code of Practice for Internal Audit in Local Government*.

We are pleased to report that we were able to place reliance on internal audit's work. Since the prior year, SWAPs computerised working paper system has been adopted. We note that this has resulted in a significant improvement in relation to the level and quality of audit documentation recorded within their electronic files.

Even though we recognise that significant improvement has been made in the quality of internal audit's work compared to last year,

particularly around the IT work and testing, we still had to perform some additional top up testing in order to gain the level of assurance required.

There are a number of improvements that could be made to further enhance the quality of internal audit's work and reduce the level of top up testing we are required to complete to satisfy our audit requirements. We have fed back our comments and details of these areas to internal audit and will continue to work closely with them.

These areas have been discussed with the Head of Internal Audit. A recommendation has been raised in **Appendix 1**.

From April 2013, 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 further improvement in the professionalism, quality, consistency and effectiveness of internal audit across the public sector. The PSIAS replace the *Code of Practice for Internal Audit in Local Government*. Additional guidance for local authorities is included in the *Local Government Application Note* on the PSIAS.

SWAP has undertaken a self assessment in relation to its compliance with the PSIAS requirements which was externally validated by the Head of the Devon Audit Partnership. The findings of the assessment revealed that there were no areas of non-compliance, but highlighted a number of areas for further improvement.

We have considered these findings as part of our separate review of internal audit which as we have previously mentioned will be reported separately to you.

The controls over all of the financial systems are sound.

However, there are some weaknesses in respect of journals and the documentation of reconciliations.

We still need to complete our testing in relation to the housing rents system.

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.

Our audit approach for grant income, payroll and non-pay expenditure remains the same as last year. We do not perform detailed controls testing in these areas as we believe them to have a low risk of material misstatement. This assessment is on the basis that there is a level of high volume of low value transactions, with a low level of complexity and with a low level of judgement involved, as well as good coverage by internal audit.

Detailed audit work on these account balances will be completed during the final audit which will focus on substantive analytical procedures.

Key findings

Based on the work of your internal auditors, the controls over all of the financial systems are sound. We noted some weaknesses in respect of individual financial systems that may impact on our audit:

- **Journals:** We identified instances where an independent review of journals was not being undertaken appropriately. In addition, we identified that some SAP users had the ability to post journals

despite their role not requiring such access.

- **Reconciliations – Documentation:** Our review of the processes in place in relation to the reconciliation between Northgate and Civica identified that it is not formally signed off so as to evidence reviews undertaken.
- **Reconciliations – Investigation:** In relation to the periodic reconciliation of the Northgate system to Valuation Office Agency Reports we identified instances where variances had not been adequately investigated, or where the investigation had not been documented.

Recommendations for journals and reconciliations have already been identified and made by internal audit and we are therefore not repeating them in this report.

We have not yet completed our assessment of the controls over housing rents and financial reporting. Due to the implementation of the QL housing rents system there were a number of controls which, at the time of our onsite work, were still being developed. In addition, some of the financial reporting controls are performed on an annual basis as part of the preparation of the accounts. We will undertake the required work in relation to these areas as part of our final audit visit in July 2013.

Financial system	Assessment
Financial reporting	TBC
Journals	Effective
Fixed Assets	Effective
Cash	Effective
Council Tax	Effective
National Non-Domestic Rates	Effective
Housing Rents	TBC

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

The Authority has made significant progress in relation to the recommendation in our *ISA 260 Report 2011/12*.

Work completed

We issued our Accounts Audit Protocol to your Chief Accountant on 20 March 2013. 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 have had further discussions with the finance department on the details within our Protocol.

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 Authority's progress in addressing the recommendations in our *ISA 260 Report 2011/12*.

Key findings

We consider that the overall process for the preparation of your financial statements is strong. Over recent years the Authority has managed the year end close down process very well and we do not anticipate any change to it this year.

The Authority has made significant progress in implemented the recommendation raised in our *ISA 260 Report 2011/12* relating to the financial statements in line with the timescales of the action plan.

No high priority recommendations were raised in our *ISA 260 Report 2011/12*.

The Authority has a good understanding of the key 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 Statements Audit Plan 2012/13*, presented to you in March, we identified the key risks affecting the Authority's 2012/13 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 your Director of Finance as part of our regular 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 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 below provides a summary of the work the Authority has completed to date to address these risks.

Key audit risk	Issue	Progress
	<p>As at March 2013, the Authority was forecasting that it would deliver an overspend against its 2012/13 budget by approximately £1.2 million. However, the Authority had plans in place to reduce the over spend by the end of the financial year in order to meet budget. The budget included a savings programme totalling £33 million and a drawdown of £1.7 million from the General Fund Reserve.</p> <p>The Authority also estimated that another £28 million in savings would need to be achieved during 2013/14, and a further £23 million in 2014/15, to address the ongoing reductions to local authority funding. Against a backdrop of continued demand pressures in Adult Social Care and Children's Services it will become more and more difficult to deliver these savings in a way that secures longer term financial and operational sustainability.</p> <p>If there are any related liabilities at year end, these will need to be accounted for in the 2012/13 financial statements as appropriate</p>	<p>We have reviewed the Authority's budget monitoring processes, including the way in which performance against savings plans is monitored. This work identified no weaknesses and confirmed that both members and officers are actively engaged in the management of the savings plan.</p> <p>As part of our VFM work we will review the Medium Term Financial Plan to ensure that this has taken into consideration the potential funding reductions and that it is sufficiently robust to ensure that the Authority can continue to provide services effectively. We will also review how the Authority is delivering its savings plans.</p> <p>As part of our final accounts audit we will review the Authority's assessment of any potential liabilities arising from its savings plans against the <i>Code</i>. We will review the Authority's provisions, including the methodology, assumptions and calculations.</p>

The Authority has a good understanding of the key 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
	<p>The migration to a new Rents System (QL) required the management of a complex system implementation and the transfer of a significant amount of data into a new system.</p> <p>Interfaces with the Council's SAP system also had to be established and designed so as to operate effectively.</p> <p>If this process was not undertaken and managed appropriately, the Council would be exposed to an increased risk that rental incomes and charges are incorrect calculated and reported.</p>	<p>We have been waiting for internal audit to complete their work on data migration before we start our testing.</p> <p>At the time of this report, internal audit work is now complete and available to us for review.</p> <p>We have agreed a scoping document with the Director of Finance and we will complete our work by the time of our year end audit.</p>

VFM audit approach

Our VFM audit risk assessment and work to date has provided good assurance on the Authority'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 Authority at present and will consider this further during our final audit.

We will complete our programme of audit work to inform our value for money conclusion during our final audit visit in July. Our value for money opinion will be issued in September alongside our opinion on the Authority's accounts.

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

- | | | |
|--|--|---|
| <p>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.</p> | <p>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.</p> | <p>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.</p> |
|--|--|---|

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
1	3	<p>Internal audit review</p> <p>We have reduced the risk rating from Priority One in the previous years to Priority Three this year, as this reflects the vast improvement of the quality of internal audits work this year.</p> <p>We have a number of improvements points in relation to:</p> <ul style="list-style-type: none"> • Sample sizes and selection of samples (limited number of areas): • No performance of walkthroughs (on IT work); • No documentation on the knowledge/skills/experience of staff performing the controls tested (on IT work); • Lack of testing of database access across all systems (on IT work). <p>These requirements are clearly outlined in the Internal Audit Protocol document which has been agreed between SWAP and KPMG.</p> <p>Recommendations</p> <p>SWAP should ensure that the following points are addressed and built into their work for next years audits in order to meet our requirements under our agreed protocol.</p>	<p>Agreed.</p> <p>Responsible officer: D Hill</p> <p>Due Date: Immediate</p>

Key issues and recommendations (continued)

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
2	3	<p>SAP Change Control Documentation</p> <p>During our testing of change control within the SAP system, we were provided with evidence for changes. However, the evidence was in the form of lengthy email chains. There was no formal change request form or helpdesk tickets.</p> <p>Change requests processed in this way increases the potential risk of changes being made to the production environment which are inappropriate, have not been authorised or have not been fully tested.</p> <p>Recommendations</p> <p>We recommend that a formal change request form should be provided for each change detailing the change, back out plans and also what testing is required. It should be clearly documented on these forms who is approving the change.</p> <p>All changes should also be logged on the Authority Service Management System to ensure a full audit trail exists.</p>	<p>All system changes to the production system are and will be managed through the system manager change process. However, routine business processes which do not make changes to the application will continue to be managed in the business environment since the risk is low.</p> <p>Changes made by CGI are recorded by them, in their own service management tool ,with cross reference back to the WC change number. Wiltshire also take record of the CGI change reference.</p> <p>Responsible officer: Stuart Honeyball Due Date: 30 June 2013</p>

Follow-up of prior year recommendations

The Authority has not implemented all of the recommendations in our Interim Audit Report 2011/12.

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 2011/12 and re-iterates any recommendations still outstanding.

Number of recommendations that were:		
	Non-IT	IT
Included in original report	1	15
Implemented in year or superseded	1	3
Remain outstanding (re-iterated below)	-	12

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
1	1	<p>Protection of the production environment from direct changes - SAP</p> <p>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.</p> <p>There is also a lack of compensating monitoring controls in place to ensure that direct database access is appropriate.</p> <p>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.</p> <p>There is a risk that unauthorised changes are made to the data in the live system which remain undetected.</p>	<p>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.</p> <p>Responsible officer: Stuart Honeyball</p> <p>Date: 30 June 2012</p>	<p>Remains outstanding</p> <p>As discussed with Stuart Honeyball and Logica (through Stuart Honeyball), Logica continue to hold a similar level of user accounts at the SAP database level, principally due to the contract support model in place.</p> <p>Although Logica have an ISO27001 audit performed by an independent and appropriately registered third party (usually on a six-monthly basis), due to the nature of the certification for this standard it only equates to performing a test of design and implementation of relevant controls at Logica</p> <p><i>[continues on next page]</i></p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
1	<p>1</p>	<p>Protection of the production environment from direct changes - SAP</p> <p>Recommendation</p> <p>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.</p> <p>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.</p>		<p>Remains outstanding</p> <p><i>[continued]</i></p> <p>i.e. rather than testing the operational effectiveness of relevant controls across an extended period of time (e.g. since the last audit) – an ISAE3402 or similar style audit is not performed and is not planned for the near future by Logica.</p> <p>KPMG note this position and have considered potential effects to the planned audit approach for 2012-13.</p> <p>Management response update</p> <p>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.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
2	1	<p>Powerful User Accounts - Northgate</p> <p>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.</p> <p>This may result in the inability to attribute actions to an individual user or unauthorised persons gaining access to the system data.</p> <p>Recommendation</p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>Responsible officer: Sally Kimber/Ian Brown</p> <p>Date: 1 July 2012</p>	<p>Remains outstanding</p> <p>Allocation of the 'First Development' role allows a user full access within Northgate and it was identified that 17 separate user IDs have been assigned this access.</p> <p>One user ID (RB) is used by the Northgate third party support provider and is subject to a weekly review of use via monitoring of logs created by the application whenever the user ID is used.</p> <p>However, no other type of formal monitoring is performed over any of the other powerful user IDs.</p> <p>Management response update</p> <p>There are 13 User IDs who are currently allocated the 'First Development' job role, these being the System Owner (Ian P Brown), the members of the Revenues and Benefits System Team and members of the Applications Team. These users carry out the System Admin function for the Revenues and Benefits system and therefore require this level of access to enable them to schedule jobs, maintain parameters etc.</p> <p>Each of these users has a unique user ID (unlike the generic account) and therefore actions carried out on the system are audited. Procedures have been put in place to monitor the use of the generic account which is used by a number of users.</p> <p>Recommendation has been implemented. No further action required.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
3	2	<p>Powerful user accounts - Civica</p> <p>Powerful “system Administrator” access to Civica WebPay is controlled via assignment to the administrators user group. However, the System Administrator advised that it was not possible to generate a list of all users assigned to the administrators group.</p> <p>“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 had access to them.</p> <p>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 only. Access to the remaining accounts is restricted to a small number of ICT staff. No review of access is performed nor are passwords subject to periodic change.</p> <p>Without proper controls there is a risk that unauthorised changes to the system data could go undetected.</p>	<p>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.</p> <p>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.</p> <p>We will investigate the options around recording who has used the generic accounts on specific dates.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: December 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around powerful user access into the application level identified that the principles of this issue are still in place i.e. three nominated system admin user IDs (with no separate user ID for normal operational usage), five generic / shared user IDs.</p> <p>Management response update</p> <p>WebPay: control in place. Users were reviewed this year and a significant number disabled/revised. The system will automatically lock any account that is not used for 90 days.</p> <p>Actioned, no further action required.</p> <p>Workstation: Logins at level 20. This has now been actioned. There are now only two generic accounts that are used by the system for routine scheduled jobs. These still have passwords that expire every 90 days and these passwords have to be reset to enable these scheduled jobs to continue.</p> <p>Actioned, no further action required.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
3		<p>Powerful user accounts - Civica (continued)</p> <p>Recommendation</p> <p>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.</p> <p>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.</p>	<i>(continued from previous page)</i>	<p>Management response update</p> <p>Database accounts: Generic accounts are used by the system when accessing the DB and is set in the ODBC connections on the client pc's. It would not be possible to log who used each instance if this connection.</p> <p>No further action required.</p>
4	2	<p>Removal of user access - Northgate</p> <p>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</p> <p>If the System Administrator is not notified of all leavers in a timely fashion there is a risk that unauthorised persons may have access to the system data.</p> <p>Recommendation</p> <p>Remind all line managers of the requirement to promptly notify the System Administrator of all leavers.</p>	<p>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.</p> <p>Responsible officer: Sally Kimber</p> <p>Date: 30 June 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around revocation of access identified that 2 user accounts had not been removed in a timely manner (greater than 60 days post leave date) and 3 user accounts in relation to relevant staff leaver remained open for use.</p> <p>Management response update</p> <p>Based on the audit report from last year, a process was put into place to check users on the Northgate system to ensure their access was still appropriate on a six monthly basis. However following the completion of the most recent audit, the frequency of the checks will be amended to 3 monthly from June 2013. Recommendation has been implemented.</p> <p>No further action required.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
5	2	<p>Removal of user access - Civica</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Recommendation</p> <p>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.</p>	<p>We will undertake annual reviews of user accounts starting December 2012.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: 1 December 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around revocation of access identified that no formal process is in place either for revocation of access or regular full review of user access rights.</p> <p>SWAP sample testing identified 7user IDs that were still open for use that related to employees that had since left employment.</p> <p>Management response update</p> <p>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.</p> <p>Recommendation has been implemented.</p> <p>No further action required.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
6	2	<p>Monitoring of powerful user access by third parties - Civica</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The System Administrator confirmed that no monitoring is performed of actions undertaken by external users on either of the above accounts.</p> <p>Recommendation</p> <p>A call should be logged with the IT help desk to record when Civica have been granted access to the WebPay system.</p> <p>The System Administrator should carry out a periodic check of any changes made to the Workstation system using the Civica_comino Domain account.</p>	<p>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.</p> <p>We will look to get ODBC access (read only) to the hosted database to enable direct enquiries on activity.</p> <p>We will ensure that a call is logged with Wiltshire's IT Service Desk when 'user' access is granted to Civica support personnel.</p> <p>The Civica_comino domain account is a Windows account. It carries no application access.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: No further actions proposed.</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around monitoring of powerful user access identified that no formal monitoring process has been put into place.</p> <p>Management response update</p> <p>As per our comment last year, we are content that current controls are sufficient. Civica staff have no direct access to the application unless granted by Wiltshire. This is only enabled for support purposes and a call will be logged recording this.</p> <p>As commented last year, the Civica_comino account is a Windows login. It carries no direct system access and therefore whilst sharing the name, has no impact on the system.</p> <p>Recommendation has been implemented.</p> <p>No further action required.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
7	3	<p>Resolution of problems directly in the SAP production environment</p> <p>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.</p> <p>It was stated that taking action in the production environment only occurred where alternative actions had already been carried out.</p> <p>Despite this, there is a risk that the production environment may be negatively impacted by performing un-tested problem resolution activities.</p> <p>Recommendation</p> <p>Resolution of problems directly in the production environment should be avoided wherever possible.</p> <p>Such activities should be carried out in a non-production environment that appropriately mirrors the production environment to validate testing performed.</p> <p>This will ensure that there is no risk to the integrity of the production environment whilst performing problem resolution activities.</p>	<p>The auditors recommendations are noted.</p> <p>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.</p> <p>Responsible officer: Stuart Honeyball</p> <p>Date: 30 June 2012</p>	<p>Remains outstanding</p> <p>Although it is understood that changes are only made directly in the production environment in exceptional circumstances, there is no formal process / control in place (for example, logging of when the production environment status is changed to unlocked for direct, potentially unrecorded changes) to identify whenever direct changes could potentially occur by either Council or Logica SAP support staff allocated the relevant access to be able to do so.</p> <p>Management response update</p> <p>This is picked up through normal change procedure where this is logged in service manager and/or CGI service management tool as appropriate. We will reiterate to WC staff and CGI that there is a requirement for the formal logging of changes including exceptional circumstances where the fix is made in live.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
8	3	<p>Changes to system configuration - Civica</p> <p>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.</p> <p>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.</p> <p>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 of the system data.</p> <p>Recommendation</p> <p>All configuration changes should be logged with the service desk.</p>	<p>Considered minor risk.</p> <p>Major system changes (new interfaces / upgrades etc) are formally tested and recorded.</p> <p>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.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: No actions proposed.</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around configuration changes identified that it is still deemed to be the case by the Authority that these types of changes are not deemed necessary to be formally documented.</p> <p>Management response update</p> <p>Configuration changes are logged with service desk. However, we make these very rarely.</p> <p>The items listed as “configuration” changes in the KPMG are system setting or rules changes, so should not routinely be logged with the service desk.</p> <p>Controls in place, so no action proposed.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
9	3	<p>Password Configuration Settings - Northgate</p> <p>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.</p> <p>Recommendation</p> <p>Amend the password parameters for the "FIRST_DEFAULT" profile in line with the Council's password policy.</p>	<p>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.</p> <p>Responsible officer: Sally Kimber</p> <p>Date: 30 June 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around password configuration settings identified that this issue is still in place, with discussions ongoing with the Northgate vendor. It was also noted by the SWAP testing that a minimum number of alphabetic characters required in a users password has not been set.</p> <p>Management response update</p> <p>Northgate have made changes to the password structure to allow the use of special characters. However, there are technical issues related potential uses of characters in password structure. Alpha characters are now required.</p> <p>It is not possible to log onto Northgate without logging onto Wiltshire Council system first. This will be reviewed with IT security staff.</p> <p>Responsible Officer: Sally Kimber</p> <p>Status: Under Review</p> <p>Target: December 2013.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013
10	3	<p>Access to migrate changes to the Civica production environment</p> <p>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.</p> <p>Recommendation</p> <p>Undertake a regular independent review of actions carried out using the ICON accounts.</p>	<p>Any issues are investigated on an exceptions basis.</p> <p>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.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: No further actions proposed.</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around segregation of duty conflicts between developers and migrators to the production environment identified that this issue still exists.</p> <p>Management response update</p> <p>Data is not migrated from live to test, or versa. Wiltshire do not have access to develop Civica.</p> <p>Access to do this is held within IT, but would be controlled if ever needed to be used.</p> <p>Controls in place, so no action proposed.</p>
11	3	<p>Monitoring of scheduled jobs - Civica</p> <p>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.</p> <p>Recommendation</p> <p>Introduce a formal process for daily checks on all scheduled jobs, and for reporting and resolution of any errors.</p>	<p>Scheduled jobs are monitored on an exceptions basis. We will implement a log of 'exceptions' to include comments, resolutions etc.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: 1 December 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around monitoring of scheduled jobs identified that this issue still exists.</p> <p>Management response update</p> <p>These are monitored and dealt with on an exceptions basis. There are system logs that can be interrogated to confirm successful running, but these are not manually recorded elsewhere.</p> <p>Controls in place, so no action proposed.</p>

Follow-up of prior year recommendations (continued)

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at April 2013 date
12	3	<p>Change Control - Civica</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Recommendation</p> <p>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.</p>	<p>For WebPay (hosted), Civica are contractually obliged to provide an up to date system. Therefore they apply software patches etc directly.</p> <p>Version / functionality upgrades etc are controlled by Wiltshire and are tested and logged etc.</p> <p>A basic process for upgrades etc will be documented.</p> <p>Responsible officer: Neil Salisbury</p> <p>Date: 1 December 2012</p>	<p>Remains outstanding</p> <p>KPMG review of SWAP testing performed in December 2012 around documentation of the change management process (both of the process itself and key stages performed when a change is being made) identified that this issue still exists.</p> <p>Management response update</p> <p>Changes are managed securely and efficiently within the environment.</p> <p>Change control process is currently being documented and will be implemented.</p> <p>Responsible Officer: Neil Salisbury</p> <p>Date: December 2013</p>



cutting through complexity™

© 2013 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (KPMG International), a Swiss entity. All rights reserved.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).