West Dunbartonshire Council 2013/14

Review of Governance Arrangements and Main Financial System Report

AUDIT SCOTLAND

Prepared for West Dunbartonshire Council
May 2014

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively**.**

Contents

Introduction

1. As part of our 2013/2014 audit activity, we undertook a high level review of the governance arrangements and the main financial systems operated by West Dunbartonshire Council ("the Council"), which were identified during our planning process. The purpose of this review was to evaluate whether the Council have sound governance arrangements in place and whether the key internal controls operating within the main financial systems are adequate. It should be highlighted that these reviews were restricted to a subset of the overall controls for each system. Those reviewed were the ones we determined to be the key controls to meet our audit objectives and therefore these reviews do not represent a comprehensive review of the controls in place over any of the specified systems.

2. A listing of the systems reviewed is shown on page 5. The code of audit practice requires us to establish that controls are operating in accordance with our understanding, through discussions with officers, walkthrough tests and tests of control.

3. This report summarises the findings from our reviews highlighting, on an exception basis, where we have identified any governance issues or control weaknesses or areas where procedures are deemed adequate but could be improved further. The issues outlined in this report are only those which have come to our attention during the course of our normal audit work and are not necessarily, therefore, all of the weaknesses which may exist. It should be noted that the members and officers of the Council are responsible for the management and governance of the organisation and, as such, communication of issues arising from this audit does not absolve management from its responsibility to address the issues raised and maintain an adequate system of governance, internal control and performance management.

4. In our Annual Audit Plan issued in February 2014 we highlighted issues which could affect the financial statements of the Council. Note that these risks have not been repeated in this report unless we are of the opinion that there has been a material update which it is appropriate to comment on.

5. The co-operation and assistance afforded to audit staff during these reviews are gratefully acknowledged.

Scope

6. Our review of the Council's governance arrangements drew upon a variety of information sources including committee minute review, council reports, meetings with council officers, corporate and directorate plans and governance documentation such as financial regulations, workforce plans, scheme of delegation and standards of conduct.

7. We identified the key controls and completed walkthrough tests in the following main financial systems:

- Trade Payables (Creditors)
- Trade Receivables (Debtors)
- Main Accounting
- Payroll
- Cash & Banking
- Housing Rents
- Council Tax Billing & Collection
- Non Domestic Rates Billing & Collection
- Unified Benefits
- Council Tax / Non Domestic Rates Valuation
- Treasury Management

8. Our audit approach enables audit judgements to be based on current year testing of controls and, in accordance with ISA 330, para 14 and 15, where appropriate, prior year results. We performed an assessment of the wider control environment, and specific reviews of audit work performed in 2012/13 and concluded that reliance could be placed on certain systems based on the prior year work. Responsibility for the performance of more detailed tests of control on the remaining systems was split between External Audit and the Council's Internal Audit Team. The table below shows how responsibility for the reviews was split.

Audit Scotland	Internal Audit	Reliance on Prior Year's Testing
Cash & Banking	Non Domestic Rates Billing	Trade Receivables
Payroll	Treasury Management	Housing Rents
Council Tax Collection	Council Tax Recovery and Enforcement	Council Tax / Non Domestic Rates Valuation
Trade Payables	Main Accounting	Non Domestic Rates Collection

Summary of Main Findings

9. Overall we are satisfied that the Council's governance arrangements and internal control systems are operating as planned. The Council has made progress implementing the actions agreed in our 2012/13 Review of Governance Arrangements and Main Financial Systems report although we note that 38% of these issues have been highlighted again in this report. Of the 13 actions agreed in the 2012/13 report:
   - 7 are fully complete
   - 1 is partially complete and an updated position is reflected in this report
   - 5 are repeated (these are tagged with an (R)' in their titles within this report).

10. Areas where improvements could be made are highlighted below.

Governance

11. **Strategy for the Prevention and Detection of Fraud & Corruption** - The Council has arrangements in place to help prevent and detect fraud, inappropriate conduct and corruption. These arrangements include: a Strategy for the Prevention and Detection of Fraud & Corruption, codes of conduct for elected members and staff; and defined remits for committees. The Council's Strategy for the Prevention and Detection of Fraud & Corruption was updated in June 2013 however it is noted that it requires further revision to reflect the provisions of the 2010 Bribery Act.

Action Plan 1

12. **National Fraud Initiative (NFI) Training** - Online training is made available to those council employees involved in the NFI process. Three of the Council's registered NFI users have not completed the training and are active users of the NFI website.

Action Plan 2

13. **NFI Reporting** - A NFI progress report was considered by the Audit & Performance Review Committee (A&PRC) in December 2013. The previous progress report was considered by the A&PRC in August 2012. We would also encourage the Council to consider publicising outcomes of the NFI exercise (internally and/or externally) to demonstrate its commitment to taking action against fraud and deterring potential fraudulent activity.

Action Plan 3

Review of Internal Audit Files

14. As documented in our Annual Audit Plan issued in February 2013 we planned to place reliance on the work of internal audit in the following areas:
   - General ledger (main accounting)
   - Council tax recovery and enforcement
   - Treasury management

- Non domestic rates billing

15. We have completed our review of these internal audit files and concluded that we can place reliance upon the work performed.

Cash and Bank

16. **Bank Reconciliations (R)** – A sample review of bank reconciliations highlighted items in the Council's bank account which take in excess of a month to be posted to the Agresso financial ledger system.

Action Plan 4

17. **Bank Imprest Accounts** - The Council has 140 imprest accounts held with five different banks and a further 33 petty cash holdings which are not held in a bank. Council policy is that all imprest accounts should be held with the Clydesdale Bank unless there is no Clydesdale branch local to the department. It is also considered good practice within the Council that the accounts include the Council in their name. Testing highlighted:

- 39 accounts held by financial institutions other than the Clydesdale Bank, some of which had a Clydesdale Bank in close proximity.
- Not all bank accounts referred to the Council in their name. Eight accounts of 100 reviewed have no reference to the Council and a further two have unusual variations of the Council's name.

Due to the volume of bank imprest accounts and relatively low balances held in them, the control testing we performed was restricted. We would recommend a more detailed review of the management of imprest accounts be considered as part of the 2014/15 Internal Audit plan.

18. A comparison of the authorised signatory list held by the cash office and the individual records held by Council departments was performed on a sample of ten imprest accounts. This highlighted the following discrepancies:

- three officers on the cash office authorised signatory list were not on the department's record
- three officers not recorded on the cash office authorised signatory list, but were included on the department's record
- one officer on the cash office authorised signatory list who had not been employed by the Council for over a year.

Action Plan 5

19. **RADIUS System Administration** – The RADIUS cash receipting system has four profiles called 'System Administrator' and one called 'Temp Admin' which can be used to process system administrator functions. These accounts enable extensive system access and, as the account user is not readily identifiable, there is an increased risk of unauthorised or inappropriate access. They are mainly used to unlock IT staff user profiles however this functionality is rarely required. It is recognised that a system administration user is required, however consideration should be given to reducing the number of these accounts, allocating this access level to a named staff member and implementing monitoring controls over activity processed by that account

Action Plan 6

Trade Payables (Creditors)

20. **Exception Reporting (R)** – In 2011/12 and 2012/13 we highlighted that there was no exception reporting to identify outstanding invoices past their payment due date. The action to address this is still outstanding.

Action Plan 7

21. **Supplier Masterfile Changes** – Out of a sample of 15 supplier bank detail changes we identified two instances where supporting evidence could not be provided.

Action Plan 8

Non Domestic Rates (NDR) Billing & Collection

22. **NDR Debtor Reconciliation (R)** – A monthly reconciliation is performed between the outstanding debtor balance on the NDR Orbis system and outstanding debtor as per the Agresso ledger. Sample testing of eight reconciliations was performed. This highlighted that:
    - four were not carried out within a reasonable time of the period end. Approximately six weeks elapsed after the period end before they were performed.
    - all eight were not subject to independent review and authorisation.

Action Plan 9

23. **Orbis Super User Access** - The NDR Orbis system has a user profile called 'SUPERUSER' which can be used to process system administrator functions. It is predominantly used as a backup to four system administrator profiles used by named employees. If used the account user is not readily identifiable on an audit trail. Therefore there is an increased risk of inappropriate access by users who are aware of the account's password. Further steps should be considered to secure this profile.

Action Plan 10

Payroll

24. **Employee Validity Check** - On a monthly basis the payroll department send details of current employees to section managers throughout the Council to verify the validity of employees on the Chris21 payroll system. Managers are only asked to respond to payroll on an exceptions

basis. Nil returns are not required. This does not provide assurance that the control is being carried out as expected. Consideration could be given to reducing the frequency of the control but implementing a process whereby managers are asked for positive confirmation that there are no issues with the employee list sent to them.

Action Plan 11

25. **Accessing Own Payroll Records** - On a monthly basis a report detailing instances of payroll staff accessing their own payroll records is reviewed to ensure no inappropriate or unauthorised changes are made. It is noted that some staff have system access called "FRONTIER" which enables them to access their own records. These staff are currently excluded from the monthly review.

Action Plan 12

Information Communication Technology (ICT)

26. **Disaster Recovery Plan (DRP) (R)** - A DRP is a documented process or set of procedures to recover and protect the Council's ICT infrastructure in the event of a disaster. In 2013 the ICT department produced a high level DRP supported by several detailed procedures covering the recovery of a particular application / system. Further work to complete the supporting documentation associated with the DRP has been delayed due to competing priorities. It is also noted that the approach to disaster recovery will change upon completion of the ICT Modernisation Project and shared data centre projects.

Action Plan 13

27. **ICT Change Management (R)** - A change management process should ensure system changes are logged, assessed and authorised prior to implementation and are subject to post implementation review. We identified that overseeing of the Council's ICT change management process by a Change Advisory Board (CAB) is still to be implemented.

Action Plan 14

28. **Use of unsupported and older software** - Microsoft ended support for Windows XP and Microsoft Office 2003 on 8 April 2014; this means that if a security flaw is discovered, Microsoft have no obligation to release an update to fix it. The ICT department purchased a Microsoft Enterprise Agreement as part of their ICT Modernisation Project. Under this agreement, they are current replacing the older unsupported software products, Windows XP and Microsoft Office 2003, with the more up-to-date products of Windows 7 and Microsoft Office 2010. However, the council is still using some unsupported software. The Information Commissioner has recently warned this could become a serious problem. This risk will increase as more vulnerabilities are discovered, creating more opportunities for an attacker to exploit and potentially gain unauthorised access to systems.

Action Plan 15

Conclusion

29. On the basis of the work undertaken, we have concluded that overall, we are satisfied that there are adequate governance arrangements and controls operating within the main financial systems.

Action Plan

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
Finance & Governance					
1	11	**Strategy for the Prevention and Detection of Fraud and Corruption** The Council's Strategy for the Prevention and Detection of Fraud and Corruption requires to be updated to reflect the 2010 Bribery Act. **Risk**: Staff might not be aware of the policy on, and approach to, instances where the Council is exposed to bribery.	Audit & Risk Manager	The Council's Strategy for the Prevention & Detection of Fraud and Corruption will be updated to include mention of the Bribery Act 2010	30 June 2014
2	12	**NFI Training** Three of the Council's registered NFI users have not completed the online training package. **Risk**: Inappropriate and inefficient usage of the NFI system..	Audit & Risk Manager	Council Staff involved in NFI activity will complete the online training packages which are provided	Ongoing
3	13	**NFI Reporting** Internal and external reporting of NFI progress is limited and intermittent. **Risk**: The extent to which the NFI exercise can act as a deterrent is not maximised.	Audit & Risk Manager	Officers will consider approaches to the wider publication.	31 August 2014
Cash and Bank					
4	16	**Bank Reconciliations** Items in the Council's bank account can take over a month to be posted to the Agresso financial ledger. **Risk**: The financial ledger might not represent an accurate reflection of	Section Head Financial Administration & Control	In some cases, it is not possible to post income due to lack of information received from the source	Complete

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
		the Council's financial position.		documentation. Staff have been reminded of the importance of timely and accurate postings and asked to take every reasonable step to post within 4 weeks.	
5	17 - 18	**Bank Imprest Accounts** The Council has 140 imprest accounts held with five different banks and a further 33 petty cash holdings which are not held in a bank. Sample testing has highlighted concerns about compliance with Council practice in relation to: • the financial institutions selected to hold some of these accounts • the naming convention for accounts • discrepancies in the authorised signatory list. Consideration should be given to performing a detailed review of the management of imprest accounts as part of the 2014/15 Internal Audit plan. **Risk:** There are insufficient controls in place to safeguard Council funds held in imprest accounts.	Section Head Financial Administration & Control	A full review of the current policy will be carried out. The 140 imprest accounts will also be review to ensure the title on the account and the signatories are correct. Departments will be reminded of their responsibility to ensure they advise Finance of any changes to their signatory list Thereafter, an annual housekeeping exercise will be introduced to validate the accounts	31 October 2014

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
6	19	**Radius System Administration** The Radius cash receipting system has five user profiles which are used for system administration functions. It enables extensive system access and the staff member using it is not identifiable on any audit trail. **Risk:** Staff might have inappropriate access to the Radius system.	Section Head Financial Administration & Control	The system admin accounts will be reviewed and reduced where possible.	August 2014
Trade Payables (Creditors)					
7	20	**Exception Reporting** There are no exception reports produced to identify outstanding invoices past their payment due date. **Risk:** The Council might be subject to adverse publicity or financial penalties due to non-compliance with supplier's payment terms.	Section Head Financial Administration & Control	The section will investigate putting in place exception reports for payments processed but not paid.	30 June 2014
8	21	**Supplier Masterfile Changes** Sample testing identified instances where no documentation could be provide to support changes made to supplier bank details. **Risk:** Unauthorised or inappropriate changes to supplier bank details can increase the risk of fraud and/or erroneous payments.	Section Head Financial Administration & Control	All back up to be scanned and file in a folder on the shared drive. Creditors staff have been reminded that supporting documentation must be retained for bank/payment detail changes.	31 May 2014
NDR Billing & Collection					
9	22	**NDR Debtor Reconciliation** The monthly reconciliation to ensure the outstanding debtor on the NDR Orbis system reconciles to the outstanding debtor as per the	Section Head Financial Administration & Control	The workload within the team has now been adjusted with the aim to meet the target deadline	Complete

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
		general ledger is not always performed in a timely manner and it not subject to independent review and authorisation. **Risk:** Reconciliation errors might not be identified and corrected in a timely manner.		for reconciliation and independent review. The reconciliation and review are currently up to date	
10	23	**Orbis Super User Access** The NDR Orbis system has a 'SUPER USER' profile which can be used for system administration functions, predominantly as a backup to four named system administrator profiles. It enables extensive system access and any staff member using it is not identifiable on any audit trail. **Risk:** Staff may make inappropriate changes to the Orbis system which they will not be accountable for.	Section Head Financial Administration & Control	The role of super user is allocated to named individuals in ICT. Currently the user called 'superuser' still exists and we will consider options to either close this access, or if not possible to better monitor activity.	30 June 2014
Payroll					
11	24	**Employee Validity Check** On a monthly basis the payroll department send details of current employees to section managers to verify the validity of employees on the payroll system. Managers are only asked to respond on an exceptions basis. Nil returns are not required. **Risk:** There is a lack of accountability over employee validity checks being performed.	Lead HTR adviser (payroll)	Payroll will ensure relevant Line managers confirm changes to establishments every 6 months. This will be done in July 14 and every 6 month thereafter. "Nil" returns will be required.	31 July 2014
12	25	**Accessing Own Payroll Records** The control to review instances where staff access their own payroll	Manager of Audit & Risk	A report will be developed to allow monitoring	30 June 2014

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
		records excludes staff with the 'FRONTIER' system access permissions. **Risk:** Inappropriate amendments to payroll records might not be identified.		of all staff with full FRONTIER' system access permissions.	
Information Communication Technology					
13	26	**Disaster Recovery Plan** The ICT department has produced a high level disaster recovery plan however further work is required to complete the supporting documentation which underpins the overall plan. **Risk**: The Council might not be able to protect and/or recover their ICT infrastructure in the event of a disaster.	Manager of ICT	Underlying technology at WDC is changing and the DR plan will be produced to reflect the changing environment	30 June 2015
14	27	**ICT Change Management** The Council have not yet introduced the Change Advisory Board to oversee the change management process. **Risk:** Poorly managed system changes could impact on the stability or integrity of the Council's ICT systems.	Manager of ICT	WDC has introduced Information Technology Infrastructure Library Change Management processes and has a change manager role in place. The change management processes are a best practice framework and are not prescriptive but rather a framework to adapt. WDC	Complete

Ref.	Para.	Issue	Responsible Officer	Agreed Action	Action Date
				therefore accept this risk.	
15	28	**Use of unsupported and older software** Microsoft ended support for Windows XP and Microsoft Office 2003 on 8 April 2014; this means that if a security flaw is discovered, Microsoft will not release an update to fix it. **Risk:** Operating older unsupported versions of software may result in security weaknesses.	Manager of ICT	In addition to major investment in ICT Modernisation Project, WDC has purchased the extended support for XP	Complete