KPMG

INFRASTRUCTURE, GOVERNMENT AND HEALTHCARE

West Dunbartonshire Council

Interim management report - Information technology controls
Year ended 31 March 2011

15 April 2011

AUDIT

AUDIT ▪ TAX ▪ ADVISORY

Contents

This interim management report is presented under the terms of our appointment by the Accounts Commission.

The contacts at KPMG in connection with this report are:

Grant Macrae
Director
Tel: 0131 527 6795
Fax: 0131 526 6666
grant.macrae@kpmg.co.uk

Keith Macpherson
Senior Manager
Tel: 0141 300 5806
Fax: 0141 204 1584
keith.macpherson@kpmg.co.uk

Kerr Kennedy
Manager
Tel: 0141 300 5624
Fax: 0141 204 1584
kerr.kennedy@kpmg.co.uk

David Colin Meadley
IT Auditor
Tel: 0141 300 5882
Fax: 0141 204 1584
david.meadley@kpmg.co.uk

About this report

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

This report is for the benefit of West Dunbartonshire Council and is made available to Audit Scotland and the Accounts Commission (together "the beneficiaries"), and has been released to the beneficiaries on the basis that wider disclosure is permitted for information purposes, but that we have not taken account of the wider requirements or circumstances of anyone other that the beneficiaries.

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

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

This report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the beneficiaries) for any purpose or in any context. Any party other than the beneficiaries that obtains access to this report or a copy and chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the beneficiaries.

Summary and findings

The following is a brief overview of the purpose of this report.

Background

We have recently completed our visit in connection with the audit of West Dunbartonshire Council for the year ending 31 March 2011. During the visit we discussed with key staff the use of information technology used to support the key financial systems, in order to gain an understanding of the key IT controls. Additionally we performed detailed testing required for our audit. It is our normal practice to write to senior management on completion of assignments, setting out any observations from our work.

Scope and objectives

IT controls form an essential part of managing West Dunbartonshire Council's use of technology. There is a balance to be achieved between reducing risk and maximising efficiency. The broad objectives of the review were to perform detailed testing in accordance with our audit methodology. We evaluated the design and implementation of IT general controls relevant to key financial systems. We also tested the operating effectiveness of those controls for the period 1st April 2010 to 31st March 2011. Our work assessed the IT General Controls covering the following four areas:

- access to programs and data;
- program changes;
- program development; and
- computer operations.

The key financial systems covered as part of our work are detailed under IT background and systems. In addition we followed up on issues identified in the previous year's audit.

Approach

We obtained an understanding of the IT background, systems and risks within the IT control environment through a series of fact finding interviews with staff and management.

In the performance of the IT general controls review, our work involved discussions with key staff to help us gain an understanding of the key financial system controls, supplemented by detailed testing as appropriate.

Reporting and recommendations

We have not raised any new issues as a result of this year's audit. Of the eight issues from the previous year's management report three of this have now been fully implemented leaving five open issues.

Two of these findings have been reported as part of our interim management report as they relate to broader organisation wide controls and as such we feel merit appropriate management attention. This report details our findings which are specific to the ICT service and of limited impact to the financial statements audit. Appendix one covers those points still requiring action, while appendix two details those matters which have now been closed.

Acknowledgement

We wish to place on record our appreciation of the co-operation extended to us by Council staff throughout the course of this work.

Appendix one – Management report points action plan

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

No.	Issue	Management response	Responsible officer and implementation date
1	**Password policy** As a result of a review of the Council's Computer Password Policy, we noted that there was no specific mention of the minimum password syntax rules expected by the Council. We recommend that the Policy is updated to reflect this and that all applications in use by the Council have their password syntax rules changed accordingly. Where system limitations prevent this, dispensation should be sought from the business system owner. *(Grade three)*	User guidance on implementing strong passwords was issued and published on the intranet on 17 March 2011.	John Martin ,Section Leader ICT Connect March 2011 - complete
2	**IT disaster recovery** Following on from previous recommendations, we note that there is still no formal planning around IT Disaster Recovery ("DR"). However, a number of DR tests have taken place during the year over the various systems in use, although no formal signoff was noted. We recommend that the Council adopt a more formal approach to DR to include scheduling and documenting the process to ensure that both sides of the process (IT and Business users) are satisfied with the tested arrangements. *(Grade three)*	ICT will continue to deliver specific application DR tests in conjunction with departments. March 2012 ICT will continue to refurbish Clydebank computer room to support DR testing and failover. October 2011 ICT have included an ICT Security officer post in new structure and post holder will lead on DR plans ICT will continue to develop DR plan. March 2012	ICT Security Officer Implementation dates as detailed in the management response.

Appendix one – Management report points action plan (continued)

No.	Issue	Management response	Responsible officer and implementation date
3	**Service level agreements** Following on from previous recommendations, we note that there is still a need for formal Service level agreements ("SLAs") to be put in place. This will allow the business system owners to confirm a number of areas with ICT such as data retention, incident response times and backup requirements. We do however note that the Council's current operations are in line with industry practices and as such are most likely fit for purpose, however without formal acknowledgement from the business, this cannot be confirmed. *(Grade three)*	ICT Service Level Agreement (SLA) documents are currently with service departments for signoff. SLAs will be agreed with departments in quarter one, 2011-12.	John Martin , Section Leader ICT Connect July 2011

Appendix two – Closed management report points

No.	Issue, recommendation and priority	Management response	KPMG comment for 2011
1	**Password settings** Our testing has identified password complexity on I-World, Radius and Cyborg is not considered in line with best practice standards. There is no password complexity defined for Cyborg, with passwords issued in clear to users by the system administrator. I-World does not enforce rotation and lock out of passwords and Radius does not enforce lock out. Robust password polices should contain requirements on minimum password length, complex syntax, expiry settings, inability to use the same password and lock out after failed attempts. We recommend the Council investigate if functionality can be developed to allow a suitable password policy to de fined for the three applications which conform to the requirements specified above. In addition, for Cyborg, functionality should be developed to allow users to define their own passwords which should be recorded into the application in an encrypted format (for Cyborg, we recognise the implementation of a new payroll and HR system, due April 2010, may negate this risk). *(Grade two)*	WDC will move to new version of Radius which incorporates new functionality to lock out on 3 failed log-in attempts. The facility to lock user's accounts in the Radius Cash Receipting application where a user has had 3 failed login attempts will be part of the new functionality introduced in Version 8.2a of the Radius application. West Dunbartonshire Council are currently on Version 7 of the system and intend to be on Version 9 when this application is hosted on our behalf by the software supplier. West Dunbartonshire Council carried out testing in 2009 on the Cyborg Payroll Enhanced Security functionality provided by the software supplier to address outstanding security issues with the Payroll system. The testing carried out was unsuccessful and had an adverse impact on other parts of the application and was therefore abandoned. Feedback from other sites that had tried to implement the enhanced security functionality also highlighted similar problems with their Cyborg Payroll System. The Council has since gone live with their new Frontier Payroll system in April 2010.	We note that this issue has now been closed.

Appendix two – Closed management report points (continued)

No.	Issue, recommendation and priority	Management response	KPMG comment for 2011
2	**Data security** We note the Council have compiled a series of procedure documentation which provides guidance to staff on the approach to be followed for the encryption of sensitive data. However, the Corporate Information and Communications and Security Policy (ISP 4.5) should also be updated to reflect data encryption requirements. In addition, we note the Council have now adopted the use of encrypted USB storage devices, although we were informed unencrypted devices are still in use. We would recommend unencrypted USB storage devices be removed from use and replaced with encrypted technology. We have also been informed the Council have recently required all staff to re-sign employment contracts to meet the employment requirements for Single Status and as such have formally signed up to the Information Technology Security Policy and E-mail Internet Security Policy. *(Grade three)*	The draft version of the Corporate Information and Communications Security Policy has now been updated to include the requirements for encryption of portable devices. Guidance for encryption for users now posted on the Intranet (see encryption on the Intranet attachment) Capital bid for endpoint device control software has been submitted to lock down the use of portable devices. All new USB storage devices procured through ICT are encrypted with AES 256 Bit encryption USB sticks. 25 initial laptop encryption licenses have been procured and are currently being tested with plans to roll out to approx 250 Council laptops utilised within the organisation. From mid July 2010 a priority list of laptops is currently being collated.	We note that this issue has now been closed.
3	**User acceptance testing** Although we note improvement with the recording and approval of user-acceptance test results prior to migration of changes to the production environments, limited evidence is retained to demonstrate the sufficiency of this testing. It is recognised the responsibility for performing UAT sits with business system owners in addition to the completion and retention of test documentation. Test evidence should be provided to ICT by business system owners for all changes requiring UAT. In addition, ICT should always request for test evidence as part of the change control workflow and document rationale as to why this has not been provided. *(Grade two)*	Live Production Changes are now recorded via CCF/User Acceptance Testing Sign Off document which includes the test plans being attached and filed as the one document.	We note that this issue has now been closed.