



cutting through complexity™

East Lothian Council

Interim management report – information technology

Year ending 31 March 2012

11 June 2012



Contents

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

The contacts at KPMG in connection with this report are:

Stephen Reid

Director, KPMG LLP

Tel: 0131 527 6795

Fax: 0131 527 6666

stephen.reid@kpmg.co.uk

Ally Taylor

Senior manager, KPMG LLP

Tel: 0131 527 6813

Fax: 0131 527 6666

ally.taylor@kpmg.co.uk

Sarah Burden

Assistant manager, KPMG LLP

Tel: 0141 309 2508

Fax: 0141 204 4584

sarah.burden@kpmg.co.uk

	Page
Introduction	2
Financial systems used by the Council	3
Overall arrangements	4
Detailed findings	5
Appendix	8

About this report

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

This report is for the benefit of East Lothian Council and is made available to the Accounts Commission for Scotland and Audit Scotland (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 than the beneficiaries.

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

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.

This report summarises the findings of our work on the IT control environment and financial IT systems.

Introduction

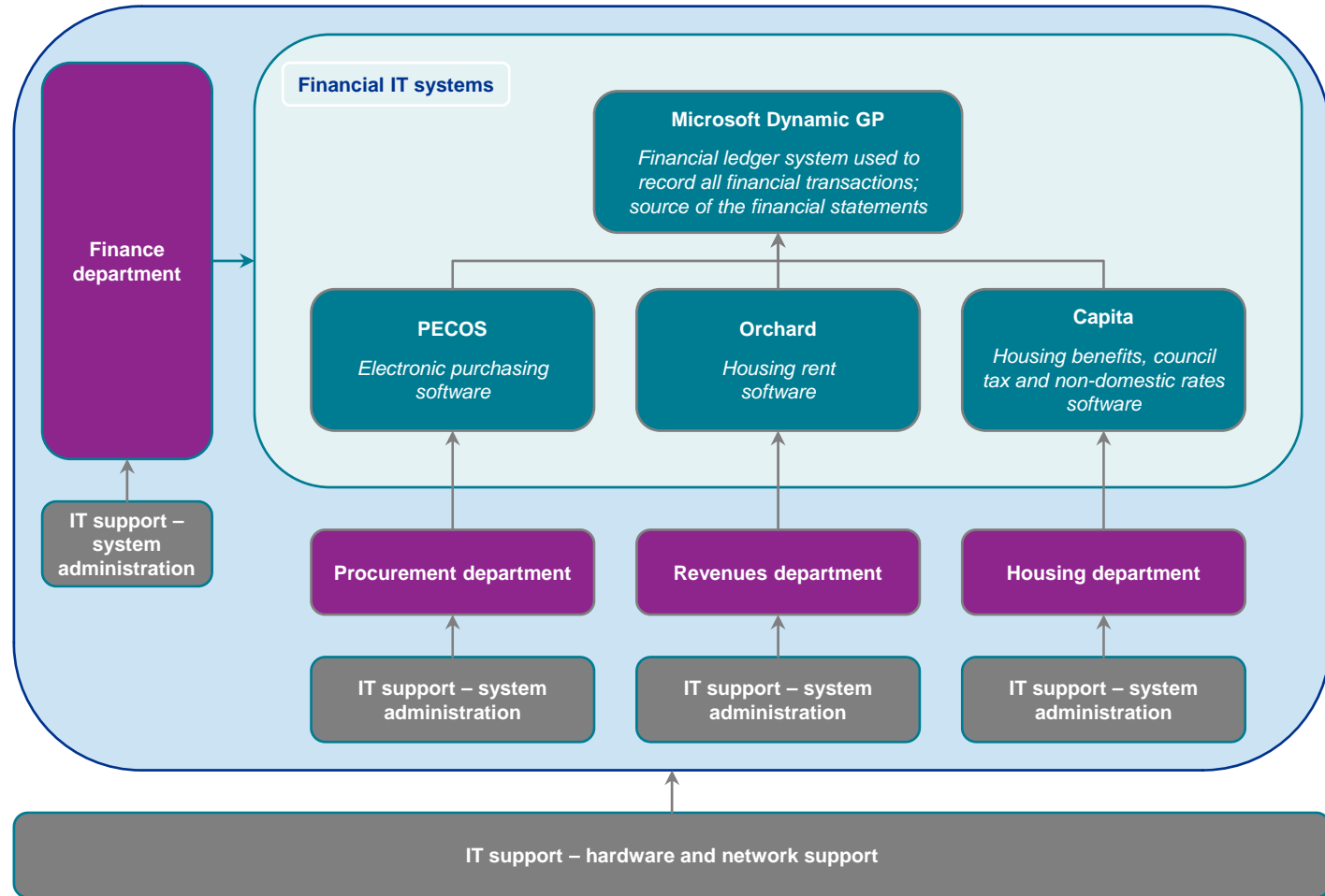
Information technology controls often have a pervasive impact on controls at the application level. IT also poses specific risks to an organisation's internal control, including:

- reliance on systems or programs that are inaccurately processing data or processing inaccurate data;
- unauthorised access to data may result in destruction of data or improper changes to data, including the recording of unauthorised or non-existent transactions;
- the possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties;
- unauthorised changes to data in master files, systems or programs;
- inappropriate manual intervention; and
- potential loss of data or inability to access data as required.

We therefore conducted an IT general controls review of key financial systems to evaluate whether these IT controls were appropriately designed and were operating effectively. The results of the review provide management with an assessment of the general IT control environment underpinning the key financial systems, the risks associated with any deficiencies identified and recommendations on how these can be mitigated going forward. Our review covered the following specific areas:

- access to programs and data;
- program changes and developments;
- computer operations; and
- end-user computing.

The diagram below summarises the financial systems and the primary departments in which they are used, along with IT support arrangements. We included all four systems in the scope of our work.




Area	Detailed findings
Structure	<p>The IT department consists of around 40 staff and the head of department reports to the executive director – support services. The department provides two services:</p> <ul style="list-style-type: none"> ▪ IT services: responsible for infrastructure and security; and ▪ IT business services: providing support to all IT users across the Council.
Change management	<p>All IT software changes are developed by third parties under service level agreements. Implementation is managed by the IT department; some upgrades are implemented with the assistance of the third party software developer.</p>
Physical security	<p>All applications are located at the Council’s headquarters and subject to expected controls, including:</p> <ul style="list-style-type: none"> ▪ restricted access to the room; ▪ CCTV coverage and a visitors log; ▪ temperature control, air conditioning and cooling systems; and ▪ smoke and heat detection and gas suppression systems.
Back-up and disaster recovery	<p>All server data is backed up regularly and stored in one of two separate locations (Haddington and Macmerry). Disaster recovery and business continuity plans exist; disaster recovery plans associated with systems classified (by management) as ‘high priority’ are tested annually.</p>

Area	Detailed findings	Action plan reference	Overall findings
Policy	<p>All new employees receive a copy of the IT acceptable use policy and must sign an acknowledgement form to confirm that they have read and understood the policy.</p> <p>The policy is being reissued to all education staff following a recent data security breach. However, there is otherwise no scheduled periodic resigning or training to ensure and enhance awareness and compliance with the policy.</p>	One	●
Policy	<p>There is no defined timetable to update the IT acceptable use policy and it has not been updated since January 2010. While our high level review of the policy did not identify any significant weaknesses, the IT environment and the way in which staff operate, continues to develop and evolve, with an ever-increasing emphasis on portable data and handheld devices.</p>	Two	●
Access	<p>The IT policy requires that system passwords are at least eight characters in length and must include special and numeric characters. We identified the following non-compliance with the policy:</p> <ul style="list-style-type: none"> ▪ the housing rent system requires only that passwords are six characters; and ▪ the over-arching Windows, financial ledger and procurement system passwords can also be six characters, with no requirement for special or numerical characters. <p>The IT policy is consistent with good practice, however the main financial systems allow staff to use passwords which do not meet the defined criteria.</p> <p>In addition, there are inconsistencies in the time required between forced password changes, ranging from 45 to 90 days.</p>	Three	●

Key: ● Significant weakness in key controls exists
 ● Weaknesses in the control process were identified
 ● No areas for improvement were identified

Source: KPMG observations during the audit.

Area	Detailed findings	Action plan reference	Overall findings
Access	<p>The human resources department provides monthly lists of leavers to the majority of systems administrators, with the exception of the revenues department. We identified a number of weaknesses:</p> <ul style="list-style-type: none"> ▪ The revenues department performs a six monthly review of housing rent system users, but none have been performed in 2011-12 due to time being spent on system upgrades. We tested a sample of leavers – provided by the payroll department – and identified four staff who no longer work for the Council, but continue to have access to the housing rent system. None of these individuals have logged onto the system since leaving employment. ▪ The procurement system and financial ledger administrators are notified of leavers, but do not retain evidence of this notification or that the member of staff has been removed from the system. 	Four	

Appendix

The action plan summarises specific recommendations, together with related risks and management's responses.

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 weaknesses 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 control to meet their objectives in any significant way. These are less significant observations than grades one or two, but we still consider they merit attention.

Finding(s) and risk(s)

Recommendation(s)

Agreed management actions

1 IT policies

Grade two (material)

There is no scheduled periodic resigning of the IT acceptable use policy during an employee's period of employment, or training, to ensure and enhance awareness and compliance with the policy.

There is a risk of complacency or a lack of awareness of specific aspects of the policy, which may result in loss of data or inappropriate use of Council IT systems and programmes. The impact of risks materialising is likely to be based on reputational damage.

Management should implement a mechanism to ensure that staff remain up to date with all aspects of the policy.

We currently operate a four year re-signing regime for our acceptable use policies. However, we will tighten this up to ensure they are re-signed every two years.

The Council have recently purchased additional licences for our online information awareness training tool to cover all staff. It is proposed that all staff will be required to undertake the training.

Responsible officer: IT services manager

Implementation date: 31 March 2013

Finding(s) and risk(s)	Recommendation(s)	Agreed management actions
<p>2 IT policies Grade three (minor)</p>		
<p>There is no defined timetable to update the IT acceptable use policy and it has not been updated since January 2010.</p> <p>There is a risk that reactive policy updates fail to prevent data loss or compromise.</p>	<p>Similar to all Council policies, the IT acceptable use policy should be subject to annual review to determine whether updates are required.</p>	<p>Both the school and corporate acceptable use policies are currently reviewed and revised if appropriate, on an annual basis. Currently, reviews are not recorded on the policy document, which only records dates when changes have actually been made.</p> <p>We will include a version control record on the policy documents to note when they have been reviewed / revised, which will continue to be annually.</p> <p>Responsible officer: IT services manager</p> <p>Implementation date: 31 July 2012</p>
<p>3 Access - passwords Grade two (material)</p>		
<p>The IT policy requires that system passwords are at least eight characters in length and must include special and numeric characters.</p> <p>The IT policy is consistent with good practice, however the main financial systems allow staff to use passwords which do not meet the defined criteria.</p> <p>In addition, there are inconsistencies in the time required between forced password changes, ranging from 45 to 90 days.</p> <p>There is a risk that passwords are not sufficiently robust, and that passwords become out of sync and staff keep a written note of their passwords.</p>	<p>Management should, where systems permit, introduce a consistent approach to forced password changes and a consistent approach to password changes.</p>	<p>IT will review the password control for individual systems with their business owners and recommend that they are brought in line with the overall IT policy on passwords wherever feasible.</p> <p>Responsible officer: IT business services manager</p> <p>Implementation date: 31 December 2012</p>

Finding(s) and risk(s)	Recommendation(s)	Agreed management actions
4 Access - leavers		Grade two (material)
<p>The human resources department provides monthly lists of leavers to the majority of systems administrators, with the exception of the revenues department. However, there is a general lack of evidence retained to evidence action. We also identified four former members of staff who still had access to the housing rent system.</p> <p>There is a risk of unauthorised access to IT systems.</p>	<p>The human resources department should notify all system administrators of leavers and these administrators should retain evidence to demonstrate that leavers have been removed from the system.</p>	<p>IT will work with human resources / payroll to identify all relevant system owners / administrators to enable the system owners / administrators to be notified of leavers. Responsible officer: IT business services manager; Implementation date: 31 December 2012</p> <p>Human resources staff will implement a business process to email the IT service desk with leaver information, as soon as a leaver is confirmed. Responsible officer: senior human resources adviser; Implementation date: 31 August 2012</p> <p>IT client teams will create and subsequently maintain a list of business system owners/administrators Responsible officers: IT client team leaders; Implementation date: 31 August 2012</p> <p>IT service desk actions - on receiving a leaver email from human resources, the IT service desk will</p> <ul style="list-style-type: none"> ▪ create a request call on the eSD service desk system ▪ allocate the eSD call to the IT infrastructure and security team ▪ email the system administrators on the list maintained by the IT client teams <p>Responsible officer: service desk and support team leader; Implementation date: 31 December 2012</p> <p>IT Infrastructure and security team action</p> <ul style="list-style-type: none"> ▪ arrange to revoke network and phone access from the end of the leaving date ▪ set the eSD call to resolved <p>Responsible officer: infrastructure and security team leader; Implementation date: 31 December 2012</p> <p>Business based, system administrator actions - on receipt of leaver information from the IT Service Desk, the systems administrator will</p> <ul style="list-style-type: none"> ▪ check whether the leaver has access to the system(s) that they administer ▪ arrange to revoke system access at the end of the leaving date if applicable ▪ maintain a record of leaver actions taken for audit purposes <p>Responsible officer: individual system administrators; Implementation date: 31 December 2012</p>



cutting through complexity™

© 2012 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).