Governance, Risk and Best Value Committee

10.00am, Thursday 3 April 2014

Internal Audit 2013/14 – Overview of internal audit follow up arrangements and status report as at 28 February 2014

Item number	8.3
Report number	
Wards	None

Links

Coalition pledges	
Council outcomes	CO25
Single Outcome Agreement	SO1

Richard Brown

Chief Internal Auditor

Contact: Richard Brown, Chief Internal Auditor

E-mail: richard.brown@edinburgh.gov.uk | Tel: 0131 469 3081

Executive summary

Internal Audit 2013/14 – Overview of Internal Audit follow up arrangements as at 28 February 2014

Summary

This report provides:

1) an overview of new internal audit follow up arrangements; and

2) status of follow-up actions as at 28 February 2014.

Recommendations

It is recommended that the Committee note the status of follow-up actions and determine which, if any officers they want to discuss the status with.

Measures of success

The success of the internal audit approach to undertaking and reporting follow up will be reflected in the percentage of actions fully implemented within the timetable agreed and where not agreed Committee can determine whether action to date is acceptable or further action required.

Financial impact

Not applicable.

Equalities impact

Not applicable.

Sustainability impact

Not applicable.

Consultation and engagement

The approach was agreed with the Head of Legal Risk and Compliance and Director of Corporate Governance. An overview was provided at the Corporate Management Team (CMT) and each Director was made aware of responsibilities to implement and agreed internal audit recommendations.

Background reading / external references

Not applicable – Approach in line with CIPFA IA Code of Practice.

Report

Internal Audit 2013/14 – Overview of internal audit follow up arrangements as at 28 February 2014

1. Background

1.1 It was reported to committee on 10 October 2013, that new procedures had been introduced for escalation of issues to CMT and GRBV, where follow-up actions have not been taken by management in relation to critical, high and medium risks.

1.2 The revised procedures are:

1.2.1 All internal audits with any findings are followed up between 4 and 9 months after the issuance of the final audit report.

1.2.2 Internal audit verify with management whether all actions have been implemented and require supporting evidence.

1.2.3 A formal follow-up report is sent to management highlighting the status of follow-up actions, in particular highlighting those that have not been implemented.

1.2.4 A report is taken quarterly to CMT and GRBV highlighting all critical, high or medium risk actions where no implementation of recommendation has occurred.

1.3 This is the second quarterly report reflecting the new escalation procedures.

1.4 In addition this report provides, at Appendix 1, a status report on follow up at 28 February 2014

2. Main report

<u>Internal Audit Follow up – overview</u>

2.1 Internal Audit follow up on a routine basis agreed internal audit recommendations. Each recommendation agreed has an allocated responsible Officer and a date for implementation. Internal Audit seeks confirmation from each Officer over how the action has been implemented and is asking for formal evidence that action has taken place.

2.2 A formal follow-up report is produced at the end of the follow-up audit and this is sent to senior management highlighting which actions have been implemented and which have not. This report allows management to understand the risk categorisation of the finding. Any actions which are deemed critical, high or medium risk and where actions are still outstanding, are highlighted to CMT and GRBV on a quarterly basis.

Internal Audit recommendations – status of "overdue" recommendations as at 28 February 2014

2.3 A detailed analysis of follow up reviews where internal audit issued high and medium risk agreed actions and the implementation date agreed has now passed is included at Appendix 1. This was the status as at 28 February 2014 and will be refreshed as implementation occurs.

3. Recommendations

3.1 It is recommended that the Committee note the status of follow-up actions and determine which, if any officers they want to discuss the status with.

Richard Brown

Chief Internal Auditor

Links

Coalition pledges	
Council outcomes	CO25 - The Council has efficient and effective services that deliver on objectives
Single Outcome Agreement	SO1 - Edinburgh's Economy Delivers increased investment, jobs and opportunities for all
Appendices	Appendix 1 – Status report

Internal Audit 2013/14 – Overview of internal audit follow up arrangements as at 28 February 2014
Appendix 1 – Outstanding Recommendations, Detailed Analysis

No	**Department & Review Title**	**Outstanding Issue / [Risk]**	**Risk Level**	**Action Status**	**Current Position**	**Responsible Officer(s)**	
	CORPORATE GOVERNANCE						
1	**Network Access Control**	There is no CEC Network Access Control policy or defined responsibility for the Windows Active Directory user validation	High	Not implemented	An updated 'Information Security Policy Countermeasures' document incorporating Network Access Control is under development and will be submitted for approval in due course.	Chief Information Officer	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
2		It is normal practice for organisations to base their licensing on Active Directory user data however given the current state of Active Directory this is not possible. CEC us an ‘as per physical asset’ method, based on BT Hardware Asset register which is known to be inaccurate. A means for preventing it becoming out of date has not been established	Medium	Not implemented	Significant progress has been made in relation to implementing this recommendation; however some obsolete/historical/redundant data has still to be removed.	Chief Information Officer	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
3		The BT Local Work Instruction (BTWI) covering the reset of an Active Directory Password states 'If a manager requires to reset the password of an employee they must email the details of the employee and 'the BT operative must check that the employee is managed by the requestor' under the organisation tab in Active Directory, if this doesn't match advise the user we are unable to confirm management chain and unable to reset. Current practice is for the user requiring unlock/reset to make a helpdesk call and the password can be reset without identity being checked.	Low	Not Implemented	Evidence of communication with BT provided but no evidence of resolution being reached. No evidence of BTWL being amended or any agreement on adherence	Chief Information Officer	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
4		Active Directory contains 5797 accounts which have not been use for more than 3 years and 899 accounts not used for over 6 years. 2083 have never been used. There is evidence of obsolescence in 'post refreshed' accounts already	High	Not implemented	A Request for Change was submitted to BT in May 2013 to action a clean-up, however this has yet to be fully completed and no evidence provided on agreed disable and delete criteria going forward	Chief Information Officer	
5		Inconsistent use or completion of Active Directory data fields. Some non-employee accounts have very little detail recorded making difficult to verify whether the account is required or not.	Medium	Not implemented	Email evidence was obtained detailing some consideration of account types with BT, however no evidence was provided as to the final outcome and/or required mandatory fields	Chief Information Officer	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
6		Active Directory is structured into Organisational Units (OU). It is apparent that Active Directory reflects the current CEC structure of 2005, prior to the Departmental reorganisation. This is also the case for the refreshed network user accounts.	Low	Not implemented	Received a copy of the RFS submitted in 2013 however there has been no update on the implementation of this amendment	Chief Information Officer	
7		Non-employee, admin, test and training accounts have logon names of varied lengths and formats.	Low	Not implemented	Email evidence was obtained detailing some consideration with BT, however no evidence of implementation was available.	Chief Information Officer	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
8		Of the 207 leaver accounts still active, 105 show activity after the employee leaving date. 4 of these employees were dismissed.	High			Chief Information Officer	
		All leavers should be notified to BT and dismissed staff should have their access revoked immediately		Not implemented	No implementation evidence provided.		
		Where accounts are to be used by colleagues to retrieve business data from leavers files after they have left, this should be noted in the Active Directory notes so it is clear who is using the account.		Not implemented	Email evidence of the issue being raised within new accounts removal process/LWI was obtained however no copy of the removal process/LWI was provided.		

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
9		CEC have a leaver's form covering employees paid through payroll which reminds management of their responsibility to arrange leaver's access to be revoked. There is no leaving form covering agency/contract staff. It is known that BT are not always notified of users leaving and the lack of a master listing of all agency/contract staff precludes retrospective checking.	Medium	Not implemented	A proposal has been submitted to Organisational Development on a solution to control weakness however no information of the outcome or implementation available at the time of follow up.	Chief Information Officer	
10	**Cash & Cash Equivalents**	Localised procedures held within each team, but there is no central policy in place which can be applied across the Council.	High	Not implemented	BCM are working with Treasury re: bank account reconciliations covering all areas of the council as Treasury are involved in the wider cash and banking controls plan	Banking Control Manager	
11		Of the Council's 12 main bank accounts 4 of the related bank reconciliations were not subject to secondary review.	Medium	Not Implemented	in progress – completion expected after meeting postponed into 2014	Banking Control Manager	

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
12		2 accounts the reconciliation documentation could not be provided to us due to the absence of a member of staff - Restricting the operation of a key control to one member of staff significantly increases the risk that the control will not operate in the absence of that staff member	Medium	Not Implemented	Not completed (in progress – finalisation of procedures showing this is expected in January after postponed 16/12/13 meeting).	Banking Control Manager	
13		Review of cash related suspense accounts, found that there were 5 expenditure suspense accounts used to process statement billing which were not subject to a formal programme of regular review.	Low	Not Implemented	A formal review of the utility billing accounts has been established and documented procedures are to be prepared by the end of December. The purchase card account is being reviewed regularly, the processes for Purchase Cards are currently being reviewed, which means that arrangements have not yet been formalised. This is due to restructuring within the Payments unit and staff changes which have raised issues.	Banking Control Manager	
	SERVICES FOR COMMUNITIES						

No	Department & Review Title	Outstanding Issue / [Risk]	Risk Level	Action Status	Current Position	Responsible Officer(s)	
14	**Accounts Payable Feeder Segregation of Duties Review**	CEC system administrator can access Tranman files held on a local server. This includes files containing payment details - Payment file changes could be made and go undetected.	High	Not implemented	At this stage management are comfortable that only 2 senior members of staff have access to this information and there has been no issue in 14 years. Management accept the risk. It will be examined in any future upgrade of the system.	Contracts Manager Waste & Fleet Services	
15		The test system allows CEC system administrator to order and approve related payments	Medium	Not implemented	Management accept the risk.	Contracts Manager Waste & Fleet Services	
16		One administrator user ID and password used by two CEC employees and the third party vendor.	Medium	Not Implemented	Management accept the risk.	Contracts Manager Waste & Fleet Services	
17		Tranman system administration password is only four characters in length with no forced complexity. Current Council policy is for passwords to be a minimum of eight characters with complexity forced by the system.	Medium	Not Implemented	Management accept the risk.	Contracts Manager Waste & Fleet Services	

No	**Department & Review Title**	**Outstanding Issue / [Risk]**	**Risk Level**	**Action Status**	**Current Position**	**Responsible Officer(s)**	
18		User password complexity is inadequate in that a password can consist of any six characters.	Medium	Not Implemented	Management accept the risk.	Contracts Manager Waste & Fleet Services	