IT risk assessment

Blackburn with Darwen Borough Council

Audit 2010/11

The Audit Commission is an independent watchdog, driving economy, efficiency and effectiveness in local public services to deliver better outcomes for everyone.

Our work across local government, health, housing, community safety and fire and rescue services means that we have a unique perspective. We promote value for money for taxpayers, auditing the £200 billion spent by 11,000 local public bodies.

As a force for improvement, we work in partnership to assess local public services and make practical recommendations for promoting a better quality of life for local people.

Contents

Introduction

1 As part of our annual opinion audit we assess the control environment within which the financial statements are produced. Within this process we carry out a risk assessment of the IT control environment in which the financial systems are processed. Our audit approach includes a consistently structured IT risk assessment, which we use across all our audited bodies.

2 On the basis of our risk assessment of the IT control environment we form a judgement as to whether we can rely on software controls within the financial systems.

3 Where there is a high risk of weaknesses in the IT control environment we decide what changes we need to make to our financial system testing approach to mitigate the risks.

Background

4 We carried out our IT risk assessment at Blackburn with Darwen Borough Council in December 2010 and January 2011. Our assessment findings are based on:

- meetings with officers from IT and finance;
- meetings with Capita payroll staff;
- liaison with Internal Audit;
- review of documents; and
- testing of the design and operation of controls.

5 Last year we assessed the Council's IT control environment as high risk because of security issues around Government Connect, the IT transformation agenda and the lack of assurance on the adequacy of the IT general controls applied by Capita. We have followed up the progress made by the Council on these issues as part of this year's assessment.

Summary findings

6 We have seen a noticeable improvement in the Council's IT control environment this year. Our overall assessment of the control environment is low risk. This means we are able to rely on software controls within the financial systems. Overall we consider that adequate corporate IT controls are now in place.

7 Nonetheless there are still a number of areas where there is scope for further improvement where procedures and processes still fall short of recognised best practice. Some issues will be addressed once the Council moves to its purpose built data centre during 2011. In any event the Council could do more to improve the coverage and profile of its IT security policy and strengthen access controls, particularly within application systems.

8 We have set out in our report several recommendations which we consider should further enhance the improvements the Council has made in the last year.

Corporate IT controls

Control objectives

- Organisational policies and management procedures are in place to enable the IT function to be properly controlled. Management and staff are aware of their duties and responsibilities.
- Incident and problem management procedures provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.
- IT risks are identified and managed.
- Internal IT audit work is of adequate coverage and quality.

Key findings

9 The structure of the Council's IT team (BT&IT) provides for adequate segregation of system development duties from the operation and technical support of live systems. The line management structure and the use of corporate performance monitoring procedures provide adequate supervisory control. A cultural change within the section was evident, with staff noticeably more confident that they are allowed to discuss with the auditor areas where improvements are needed.

10 The Council's IT strategy continues to provide an appropriate framework but, as noted by Internal Audit, the more detailed documentation supporting its implementation ('roadmap') needs to be more effectively kept up to date.

11 IT security policy is more fragmented and less comprehensive than seen at most unitary authorities. There is scope for including improvements to IT security policy within a wider programme to raise the profile of information security across the user community.

12 The Council's IT service desk system is not as closely based on modern best practice IT service management standards (ITIL) as many that we have seen. Consequently it is not designed around the concept of logging and prioritising calls and issues as potential IT 'incidents' (losses of IT service). However, IT officers manage to work around this and we do not consider this to be a major issue.

13 Adequate arrangements are in place for addressing IT issues within the Council's risk management arrangements and Internal Audit programme. We note that technical IT audit services are no longer bought in by Internal Audit and that an in-house team member is part way through IIA computer audit training. This may temporarily reduce the technical component of the programme and Internal Audit will need to maintain a view of the key IT risks and its ability to address them.

Recommendations

There is scope for improving the coverage and profile of the Council's IT security policy. This could form part of a wider programme to raise the profile of information security across the user community.

Access controls

Control objectives

- Access to network servers, applications, programs, databases and systems tools is restricted to authorised personnel only and prevents:
  - destruction or improper changes to data, recording unauthorised, non-existent or inaccurate transactions; and
  - break down of segregation of duties by personnel gaining access privileges beyond those they need.

Key findings

High privilege access

14 We looked at control over high privilege access, both to IT facilities and within systems.

15 High privilege ('admin') access to servers is restricted to the appropriate technical team within IT but there is scope for more precisely restricting it only to the officers who need it to do their job. The extent to which this will be feasible is, however, dependent on roles and specialisations proposed in IT restructure plans.

16 A relatively large number of staff have full access to both Masterpiece and Payroll, particularly the latter. There is scope for review and fine-tuning of privileges. Full access to the Payroll system also gives access to facilities for amending data tables and processing rules, increasing the importance of restricting this level of access on a more precise assessment of need. Where IT staff need to be given full access to live application system facilities for support purposes this should be granted and revoked under change control as part of the documented response to a specific change or incident.

Password controls

17 We looked at password controls to both the network and the systems.

18 Most aspects of network passwording are adequate. Lock-out period after repeated incorrect attempts (one minute) protects against automated guessing attacks but is less stringent than usual and should be reviewed.

Starters and leavers

19 There is scope to more effectively manage the removal of the access rights of leavers. As found at many councils, although there are procedures for line managers to promptly inform IT and system administrators about leavers, the procedures are not used consistently. IT make use of a monthly HR report to remove access to the network but the report is not used by the system administrators we sampled (Masterpiece and Payroll). The removal of leavers' access rights from systems was less prompt than we have seen at most similarly sized councils, particularly on Masterpiece.

Remote access

20 Control over remote access has been improved since last year by removing remote access privileges where there is not an agreed business need. As is recognised by IT, procedures could be further brought up to recognised good practice by requiring use of a physical token to remotely access the network ('2-factor authorisation'). We understand this is planned following the implementation of the new data centre.

Recommendations

Some aspects of access control need to be strengthened, particularly within application systems.

In particular, there is a need to make improvements in:

- *removing leavers' access rights; and*
- *more precisely restricting high privilege access rights on a needs basis.*

Data centre controls

Control objectives

- Adequate arrangements are in place for the recovery of key systems from back-ups.
- Controls provide reasonable assurance that computer equipment, storage media, and program documentation is protected from environmental threats and physical access is restricted to properly authorised individuals.
- Financial reporting systems and subsystems are appropriately secured to prevent unauthorised use, disclosure, modification, damage or loss of data.

Key findings

21 It is unclear whether the Council has received any formal assurances from Capita about the controls Capita has put in place over the IT environment in which they process the Council's payroll system (We understand from Internal Audit that some reliance can be placed on work commissioned from Grant Thornton as part of an Internal Audit programme 'a few years ago' but we do not have details of the coverage, currency or findings).

22 The Council's existing data centre was not purpose built and is recognised as not fit for purpose (eg, access controls are basic, power contingency is limited and there are historical problems of flooding). Those issues are not considered further as the Council expects to be starting the move into a purpose built data centre during 2011.

23 Adequate procedures for scheduling back-ups and monitoring their successful completion are in place. However, until the move to the new data centre, the Council continues to be at risk of irretrievable loss of data or prolonged loss of services in the event of an IT disaster. Back-up tapes are stored locally, the ability to fully recover systems from them is not tested and there are no contractual arrangements to assist with recovery (eg supply of accommodation, equipment or expertise).

24 At many authorities, disaster recovery arrangements are considered together with technology developments, particularly the moves towards virtualising systems (multiple systems on a reduced number of physical servers) and storage area networks. We understand that to be the case at Blackburn with Darwen BC and that improvements to disaster recovery arrangements are planned as an integral part of the technology changes that form part of the move to the new data centre.

25 In view of the errors noted in 2009/10 in the Council's submission to Government Connect, we reviewed progress on the weaknesses identified last year as well as Internal Audit's work on this area. Although there is still scope for improvement in some areas covered by the CoCo submission (eg VPN 2-factor authorisation) the submission process is assessed as now under adequate management control.

26 Annual penetration testing of the network by external specialists identified some issues (as it does at most authorities) but we assess the issues as relatively minor.

27 Some virus infections are still being encountered on older PC equipment but the arrangements for identifying and isolating infection are adequate.

Recommendations

Disaster recovery arrangements need to be strengthened. The Council should seek formal assurances from Capita about the controls it has in place over the IT environment.

Program change controls

Control objectives

- Polices and procedures for program changes have been agreed to ensure that changes to operating systems and application systems are authorised, tested, approved, properly implemented and documented.
- In-house developments are authorised, tested, approved, properly implemented and documented.
- New or changed packaged systems are authorised and appropriately tested before being moved to live user environment.

Findings

28 As part of our IT risk assessment we assessed control over changes to a sample of the Council's main financial systems - the Masterpiece and Payroll systems.

29 The Council implemented a significant upgrade to its Masterpiece system during 2010/11 (the Fimis 4.0 upgrade). At the time of our assessment , the most recent upgrade to the Payroll system was in March 2010 to reflect legislative changes only, ie not a major upgrade.

30 We assess the control over changes to application systems to be a relatively strong area for the Council with adequate change management arrangements in place for authorisation, testing and handover.

Recommendations

None.

Appendix 1 Summary of recommendations

Table 1: **Key recommendations**

Recommendation	Officers' comments
Corporate IT controls	
There is scope for improving the coverage and profile of the Council's IT security policy. This could form part of a wider programme to raise the profile of information security across the user community.	IT security policy will be reviewed during 2011/12. The transfer of Information Governance & IT will also facilitate a comprehensive review of Information Governance as a whole.
Access controls	
Improve procedures for removal of leavers' access rights from applications, particularly on the Masterpiece system.	ICT currently receive a monthly leavers report from Payroll. This will be shared with the Finance systems. ICT are working to redesign the leavers process with HR to assure more timely and accurate information is provided.
Restrict high privilege access rights on the basis of need at both network and application level but particularly on the Payroll system.	High privilege access rights will be reviewed as system improvements to Masterpiece and Payroll take place during 2011/12.
Data centre controls	
Improve data centre environmental controls (expected to be part of the move to the new data centre).	A new data centre was handed over to the Council on 31 March 2011. A phased programme of implementing and upgrading the Council's ICT infrastructure has commenced and will be completed by 31 December 2012. This will lead to an improvement in environmental contracts as the new data centre is already classified as Tier 2 N+1.
Strengthen disaster recovery arrangements (expected to be dependent on the move to the new data centre).	As part of the move to the new Data Centre back up files of critical master data will be held at a secondary location along with limited server capacity so that if necessary critical services can continue to be delivered.
Ensure the Council has adequate assurances over Capita's arrangements for controlling the IT environment in which the Council's payroll system is processed.	This will be addressed by HR as part of the implementation of the new payroll system.

If you require a copy of this document in an alternative format or in a language other than English, please call:
0844 798 7070

Design and production by the Audit Commission Publishing Team.

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to non-executive directors, members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/member or officer in their individual capacity; or
- any third party.

Audit Commission

1st Floor
Millbank Tower
Millbank
London
SW1P 4HQ

Telephone: 0844 798 3131
Fax: 0844 798 2945
Textphone (minicom): 0844 798 2946