


Final Internal Audit Report 2010/11

London Borough of Hammersmith and Fulham Powersuite Application September 2011

This report has been prepared on the basis of the limitations set out on page 11.

This report and the work connected therewith are subject to the Terms and Conditions of the Supply Agreement dated 25 April 2008 between London Borough of Hammersmith & Fulham and Deloitte & Touche Public Sector Internal Audit Limited. The report is confidential and produced solely for the use of London Borough of Hammersmith & Fulham. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Introduction	<p>As part of the 2010/11 Internal Audit Plan, agreed by the Audit Committee on 23 March 2010, we have undertaken an internal audit of the Powersuite application.</p> <p>This report sets out our findings from the internal audit and raises recommendations to address areas of control weakness and / or potential areas of improvement.</p> <p>The agreed objective and scope of our work is set out in the Audit Brief issued on 07 March 2011.</p>
---------------------	---

Audit Opinion & Direction of Travel	None	Limited	Substantial	Full
				

Key Findings	Key Statistics & Benchmarking
<ul style="list-style-type: none"> • The password table is securely protected and access to the system tables is restricted to HFBP staff only; • Controls exist over the timeliness of inputs to the system; • A formal change control process has been established to coordinate technical changes on the system; • Powerful access to the system is shared by more than one staff member; • Password controls are generally weak on the system; • Reporting has not been adequately developed and as a result, exceptions are currently not reported; • Roles are not adequately segregated on the system; and • Accuracy controls are not adequately programmed on the system. 	<ul style="list-style-type: none"> • There are eight modules to the Powersuite application. The Council uses the Trade module only; • This module handles the Duty of Care management, Invoicing, Renewals and all types of chargeable services. Being workflow based they are embedded with best practice and can be easily tailored to meet specific needs of the operation; • There are now over 20 Councils in the UK using the Powersuite Waste Collection module; and • The annual budget spend on the support of the system is £4,200 and there are four licences (one licence for HFBP and three remaining licences for the Commercial Waste section).

Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
			Priority 1	Priority 2	Priority 3
Access Controls			2	2	1
Data Input			0	1	0
Data Processing			0	1 (See Rec 4)	0
Output Controls			0	0	0
Interfaces			0	0	0
Management Trail			0	1 (See Rec 4)	0
Backup and Recovery			0	0*	0
Support & Change arrangements			0	0	0

*Management is aware of control issues with Disaster Recovery & Business Continuity Planning. These are in the process of being set up and therefore no recommendation has been raised.

Please refer to the attached documents for a definition of the audit opinions, direction of travel, adequacy and effectiveness assessments and recommendation priorities.

Summary of Findings

Access Controls

Controls were found to be in place for the security of the system tables as users cannot change or access settings and the password recorded in the password tables are encrypted. However, access control could be improved on the application. Recommendations have been raised in relation to the need to grant individual access to the system; the need to undertake a general review of user permissions and segregation of duties and the need to include HR in the leaver notification process. Logical access controls could also be improved as passwords are generally weak.

Data input

Controls were found to be in place with regards to the reconciliation of invoices sent to IT for printing. Source documents are also securely retained. However, we have suggested that accuracy controls be improved on the system to limit inaccurate data input and to ensure that exceptional instances be reported so that they can be reviewed.

Data Processing

Controls are in place to help ensure that the Powersuite data is processed accurately. This includes the use of sequentially generated client transaction numbers that are automatically allocated to every batch invoice created onto the Powersuite application. These are time and date stamped. Although changes to standing data (for instance charge rates) were found to be properly authorised, we have recommended that a process be put in place to report and review critical changes on the system.

Output

Controls exist over the reconciliation of output reported from the Powersuite system for invoices that are transferred to the OLAS system. Report standards are also reasonable and meaningful.

Interface Controls

There is a manual feed between the Powersuite and the OLAS system. This is a new system that produces an output file which is manually loaded into OLAS when required. There is no automatic process feeding into OLAS or any other system.

Management Trail

The Powersuite application has an audit trail which logs the user ID of users who performed an activity on the system, the log type, the log reference, the log date and time. However, this does not report on the old charge rate.

Backup and Recovery

Although this area was included in the review there are no recommendations as management are already aware of weaknesses which exist in general with Disaster Recovery at the Council. There has been no change in this area for the Powersuite application and we found that, although controls exist over the integrity of the system and the data is backed up on a daily basis via the SQL12 server, there are no documented Disaster Recovery and Business Continuity plans. These are in the process of being set up and management are already aware that control improvements are required.

Summary of Findings Cont.../**Support and Change Arrangements**

A Change Advisory Board (CAB) has been established to ensure that upgrades, patches and releases to the application are properly authorised. The Powersuite system is currently still run as a project. We were informed that a contract will be drawn up once the implementation is finalised.

Acknowledgement

We would like to thank the management and staff of the Waste Management team and HFBP staff for their time and co-operation during the course of the internal audit.

1. Shared Account

Priority	Issue	Risk	Recommendation	
1	<p>Examination and discussion with the System Administrator identified that the HFBP Admin account is shared by seven users (from the HFBP, ENVNRSD - System Environment and Resident Services Team).</p> <p>The BDU account is also shared by two Customer and Commercial services team members.</p>	<p>Where a single user account is shared by more than one user there is limited accountability and the actions of that user account cannot be determined. Any unauthorised activity cannot be directly attributed to an individual user.</p>	<p>User access to the Powersuite application should be allocated to named individuals rather than through a generic shared account.</p> <p>Where there are license constraints and this is not possible, a system of exception reporting should be established to report on any critical changes performed with the use of the shared account.</p>	
Management Response			Responsible Officer	Deadline
<p>Agreed: However, this is not feasible as this is a licensed application and access is limited to four licenses only.</p> <p>Management will however investigate any controls in place to support this and to decide on the cost effective way of mitigating this control issue.</p>			Application Support Analyst	30/04/2011

2. Leaver Process

Priority	Issue	Risk	Recommendation	
3	<p>Although there have not been any leavers since the system went live in November 2010, a leaver will normally be notified by the user line manager and his/her account is disabled (locked out).</p> <p>It was, however, identified that the list of leavers is currently not notified by HR. There is also no functionality within the system to report users' last log-ins. As a result, the system administrators are unable to report and review to identify leavers/dormant accounts.</p>	<p>Where formal leaver procedures are not implemented, there is a risk of inappropriate access rights to the system being retained. These may be used for unauthorised activities on the Powersuite application.</p>	<p>A report should be established to report and review users who have not logged onto their accounts for more than 3 months.</p> <p>If identified, leaver accounts should be revoked immediately.</p> <p>Management should also request personnel/HR to provide a list of users who have left the Authority, and should use this list as the basis for the review of active accounts.</p>	
Management Response			Responsible Officer	Deadline
Agreed:			Application Support Analyst	30/04/2011

3. Password Controls

Priority	Issue	Risk	Recommendation	
1	<p>Testing with the System Manager identified the following:</p> <ul style="list-style-type: none"> • Passwords of one character length can be accepted by the system; • Password combination of alpha and numeric characters is not enforced; • Password age is not enforced on the system, hence passwords do not expire. As a result users have not been forced to change their passwords since the system went live in November 2010; • Previously used passwords can be recycled; • Although the option for default passwords to be force changed on first entry is manually ticked during the users creation process, this has not been made a mandatory field and can therefore be accidentally bypassed; and • The live accounts have been set to lock out users after five failed attempts. 	<p>Failure to enforce adequate logical access controls could lead to unauthorised users obtaining access to data and resources on the Powersuite system. Failure to review the number of failed access attempts also increases the risk that an unauthorised user may gain access to the system.</p>	<p>We recommend that the possibility to configure the Powersuite Application to be able to enforce the following controls should be investigated with the supplier:</p> <ul style="list-style-type: none"> • A minimum password length of seven characters; • The system should enforce a complex password, for example a combination of alpha and numeric characters; • Users should be forced by the system to change their passwords in line with the Council policy every 30 - 60 days; • A password history should be maintained to ensure that passwords are not recycled; • The option to force default passwords to be changed on first entry should be made mandatory; and • The maximum invalid login attempts for the Powersuite system should be set to three attempts. 	
Management Response			Responsible Officer	Deadline
<p>Agreed: This is a supplier issue as the parameters to configure the password settings have not been provided by the supplier. This will be investigated with the supplier. However, will change the invalid password setting.</p>			Application Support Analyst	30/04/2011

4. Audit Trail and Exception Reporting

Priority	Issue	Risk	Recommendation	
2	<p>We identified the following:</p> <ul style="list-style-type: none"> The changes to the charge rates in December 2010 cannot be reported by the audit trail facility; Although the reporting facility in place is capable of reporting exceptions, the Powersuite system is still new and reporting is yet to be exploited. Consequently, exceptions are not currently reported; A log is not produced of invalid access attempts; furthermore, these are not reviewed; and There is no evidence that the system is able to report on the before and after image of changes on the system, including master data. 	<p>Where a full audit log is not maintained there is a risk of loss of accountability for actions taken on the system. The lack of adequate reporting and review of exceptions increases the risk that unauthorised or inaccurate data entered on the Powersuite application may not be identified in a timely manner. Failure to regularly review security violations also increases the risk that suspicious activity may not be identified in a timely manner.</p>	<p>Audit logging should be adequately enabled to report the details for critical changes on the system (including the before and after image of changes). An exercise should then be carried out to identify exceptions that should be reported and reporting developed for such exceptions. Once established, a process should be put in place for the regular reporting and review of unusual activities on the system. Items to be reviewed could include, but not limited to, the following:</p> <ul style="list-style-type: none"> Report changes to user details; Report changes to charge rates; The log of violation attempts; and Rejected or missed data. 	
Management Response			Responsible Officer	Deadline
<p>Agreed. We will review the exceptions and investigate the reporting to be written including missing account reference fields. Reporting will be investigated with the supplier.</p>			<p>Performance and Systems Administrator</p>	<p>30/06/2011</p>

5. Segregation of Duties and Access on a Needs Basis

Priority	Issue	Risk	Recommendation	
2	Our audit identified that there are only two roles created on the system (system administrator and user). There is no facility on the system to report the permissions that have been allocated to the respective roles. It was also identified that the HFBP administrators also have input access to the application as well as access to the back end tables via the SQL servers.	Full access to the application increases the risk of duties being overlapped and not providing a suitable separation of duties, which can therefore be used for unauthorised activities that may compromise the integrity of the system.	The users and roles on the Powersuite system should be reviewed and additional roles created to ensure that duties are adequately segregated. Where this is not possible, adequate reporting should be established to report and review critical or sensitive changes made with the use of the system administrator accounts.	
Management Response			Responsible Officer	Deadline
Agreed			Performance and Systems Administrator	30/06/2011

6. Accuracy Controls

Priority	Issue	Risk	Recommendation	
2	<p>Testing identified the following:</p> <ul style="list-style-type: none"> The system has not been configured to mandate data entry into critical fields, for instance: names, address, post code, and these could be bypassed without warning. As a result, a new contractor input screen was validated from start to finish without the system mandating that data be entered into critical fields; There is neither a warning nor rejection message by the system on attempt to enter a duplicate invoice; and Potential errors are neither flagged nor prompted during data input, so that they can be investigated and corrected on a real time basis. 	<p>The lack of adequate input controls increases the risk of incomplete and inaccurate information and could result in wasted resources (time) used in correcting such errors.</p>	<p>Management should investigate and review with the suppliers the configuration of input data formatting, and consider establishing the following specific controls on the Powersuite application to help improve input of data quality:</p> <ul style="list-style-type: none"> Investigate all critical fields on the system and make them mandatory, or establish an exception report for the input staff to run and check errors and missing fields; Configure duplicate checks to flag and notify instances where a duplicate invoice is entered; and Activate the workflow in the system to require information validation so that potential errors can be flagged for their review and correction on a real time basis. 	
Management Response			Responsible Officer	Deadline
Agreed; to raise with the suppliers.			Application Support Analyst	30/04/2011

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system. The assurance level awarded in our internal audit report is not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Deloitte & Touche Public Sector Internal Audit Limited

London

September 2011

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England and Wales No 4585162.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Member of Deloitte Touche Tohmatsu Limited