

Final Internal Audit Report 2010/11


London Borough of Hammersmith and Fulham Spydus Library Management System

June 2011

This report has been prepared on the basis of the limitations set out on page 17

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 produced solely for the use of London Borough of Hammersmith & Fulham. Its contents should not be quoted or referred to in whole or in part without our prior written consent except as required by law. Deloitte & Touche Public Sector Internal Audit Limited will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose.

| | |
|---------------------|---|
| 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 Spydus Library Management System. The Spydus Library Management System is a third party hosted application developed by the vendor, Civica, and implemented by the South East Library Management Service (SELMS) Consortium which currently comprises of 9 members of public library authorities within the South-East region of England and includes the London Borough of Hammersmith and Fulham (LBHF).</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>In addition to the application audit, we circulated a questionnaire in order to capture the views of users on a number of areas in an attempt to establish any practical issues relating to the use of the system. A summary of the results of this questionnaire can be found in appendix A.</p> <p>The agreed objective and scope of our work is set out in the Audit Brief issued on 3 June 2010.</p> |
|---------------------|---|

| Audit Opinion & Direction of Travel | None | Limited | Substantial | Full |
|-------------------------------------|------|--|-------------|------|
| | |  | | |

| Key Findings | Key Statistics & Benchmarking |
|--|--|
| <ul style="list-style-type: none"> • Spydus Library Management System is a tool used to manage the loan, reservation and return of books and multi-media. Access is restricted to the Enquiry, Circulation and Help Modules in Spydus for the majority of staff, with adequate and effective controls built into the application for data input, processing and reporting output. • User access groups and accounts created in Spydus by the Systems Librarian and the permissions and privileges assigned were commensurate with the role of the staff within Library Services. • The Spydus Library Management System is hosted and fully managed with backup and disaster recovery provisions for all participating local authorities in the SELMS Consortium by the third party, Civica. Furthermore, on a local level, there is additional ICT support provided by the Council's partners, Hammersmith & Fulham Bridge Partnership (HFBP). | <ul style="list-style-type: none"> • The Public Libraries and Museums Act 1964, requires that local authorities provide a "comprehensive and efficient" public library service. • To assist the Council in complying with this legislative requirement, LBHF became a member of the South East Library Management Service (SELMS) partnership in 2007. • The SELMS Consortium was established in 2005 with the objective of implementing the Spydus Library Management System to enable all libraries to take advantage of interoperability and more effective management of library services within the South East of England. • The new Shepherds Bush Library was recently awarded, as a runner up in the 'Community Benefit' category by the Royal Institute of Chartered Surveyors. |

| Area of Scope | Adequacy of Controls | Effectiveness of Controls | Recommendations Raised | | |
|----------------------|----------------------|---------------------------|------------------------|------------|------------|
| | | | Priority 1 | Priority 2 | Priority 3 |
| Access Controls | | | 1 | 0 | 2 |
| Data Input | | | 0 | 0 | 0 |
| Data Processing | | | 0 | 0 | 0 |
| Output Controls | | | 0 | 0 | 0 |
| Interfaces | | | 0 | 0 | 0 |
| Management Trail | | | 0 | 0 | 0 |
| Support Arrangements | | | 0 | 1 | 0 |
| Back-up and Recovery | | | 0 | 0 | 0 |

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

Summary of Findings**Access Controls**

At the time of the audit, Spydus was supported and maintained on a daily basis for LBHF Library Services by a designated System Administrator (Systems Librarian) for user access and administration, system configuration, testing functionality and development work. However, the Systems Librarian has left the Council at the end of June 2010 and a suitable replacement has not been appointed. One priority one recommendation has been raised to address this issue.

Access to Spydus requires approval from the Deputy Head of Libraries, and user groups and accounts created in Spydus and the privileges assigned were identified to be commensurate with the roles of staff. There are two levels of access controls in place for user access into the Civica Spydus database; a username and password login for authentication with the Council network and then another set of username and password credentials to access Spydus on the desktop PC connected to the Council network, which has an installation of the Spydus client. Currently, generic network logons are used for access into the Customer Service Desks at the library sites, which has been approved by senior management, with password changes performed on a monthly basis. Access into Spydus was identified to require a unique username and four digit PIN; however, there was no system enforcement of password expiry and password history. Furthermore, there is no account lockout facility implemented for the Spydus system. Two priority 3 recommendations have been raised for consideration, review and practical implementation for the Library Service.

Data Input

All users have appropriate roles allocated and permissions assigned to input, amend and action data, such as customer information and library items (books, CDs and DVDs) in the Spydus database. The quality of the data and information managed at the Library Service is the responsibility of the librarian tasked with data input which is facilitated and ensured of its accuracy through the various data input controls in place such as, mandatory fields, table look-ups and data checks built into the Spydus system. Furthermore, the Bibliography Data Service (BDS) is used with the Spydus 'Cataloguing' module to allow dedicated staff through the use of the Z39.50 protocol to create, use and search Machine Readable Cataloguing (MARC) records which ensures records for library items are consistent in the database and compliant with bibliographic standards. No recommendations were raised in this area.

Data Processing

Controls were identified to be adequate in relation to data processing for the Spydus application with the automated, scheduled and timely processing of renewal and fine notices for the public. No recommendations were raised in this area.

Output Controls

Reports of various permutations can be produced using the 'Reports' module within Spydus for the Library services. Furthermore, this information can also be displayed using the 'Enquiry' module which is granted to the majority of users. No recommendations were raised in this area.

Interfaces

Currently, no other systems were identified to interface with the Spydus Library Management System.

Management Trail

The Spydus database maintains an audit trail for activities that are performed on the system and including all cash transactions carried out using the Cash Management function in the Spydus 'Circulation' module. Generally, information on the Spydus database can be viewed through either the Enquiry Module with drill down of borrower, transactions, charges, fee waivers and catalogue items or the 'Reports' Module in Spydus whereby reports can be generated depending on the filtering criteria. No recommendations were raised in this area.

Support Arrangements

The support and maintenance arrangements for the Spydus Library Management System are through a combination of external and in-house arrangements. There is a support agreement in place for the Spydus database with Civica who host the Library Management System for SELMS and includes technical support and maintenance with full DR provisions. The in-house arrangements are provided by the Council's ICT partners, Hammersmith and Fulham Bridge Partnership (HFBP) who were responsible for the project implementation of Spydus and are responsible for the Council's ICT infrastructure, as well as the Systems Librarian who has left the Council. At the time of the audit review, a catalogue of Spydus related technical and operational issues were logged with the HFBP, however, there was no formal handover of roles and responsibilities. One priority 2 recommendation has been raised.

Back-up and Recovery

There is 24x7 support and maintenance contract with the provision of a specialist data centre by Civica who are responsible for the maintenance, patch management, upgrades, change control, back-ups and the disaster recovery and restoration of the Spydus database for the Council. As part of the support service provided by Civica, there is also a Help Desk Service in place, as well as an online help facility and a discussion forum for Spydus users. No recommendations were raised in this area.

Acknowledgement

We would like to thank the management and staff of the Libraries and Archives / Residents' Services of London Borough of Hammersmith & Fulham (LBHF) and the Hammersmith & Fulham Bridge Partnership (HFBP) for their time and co-operation during the course of the internal audit.

1. Systems Administrator for the Spydus system

| Priority | Issue | Risk | Recommendation |
|----------|--|---|--|
| 1 | <p>At the time of the audit, it was identified that the Systems Librarian is leaving the Council at the end of June 2010 without a suitable replacement identified and recruited or appointed by senior management to be formally responsible for system administration, system configuration and user access management of the Spydus system.</p> <p>There has been no formal handover arranged for System Administration at the Library, although HFBP can provide a level of support, as defined by the business. The technical expertise and knowledge of system configuration, parameter setting and testing on Spydus requires a combination of skills of that of a qualified Librarian, as well as an in-depth knowledge of Spydus which has been lost.</p> | <p>Where a critical role in a business or service, in this case a Systems Administrator for the Spydus system, is not appointed with formal handover for the library service, there is an increased risk in the loss of key support, technical knowledge and skill, which will have a significant and detrimental impact on the business and the service to the public.</p> | <p>Management should perform an immediate and full review and evaluation of the Systems Librarian role for the Library Service with the objective of identifying and appointing a suitable replacement with a formal handover for uninterrupted continuation of the business and public library service at the Council.</p> <p>Alternatively, a review of the service in conjunction with HFBP to make suitable arrangements for an agreed level of support to be provided by Civica for specific business support for Spydus for example, one day a week.</p> |

| Management Response | Responsible Officer | Deadline |
|--|---------------------------------|------------|
| <p>Systems Librarian: Agreed. The systems librarian who has left Library Services was the first point of call for all library technical and operational issues including Spydus related issues with support from RSD. In his absence, responsibility is to be transferred over to the Deputy Head of Library Services who is to identify the Spydus related calls and discuss issues with HFBP.</p> <p>Head of Application Services and Application Support Analyst, HFBP: Agreed and a responsibility assigned to the Deputy Head of Library Services. HFBP will provide support as defined and agreed by the business owner.</p> <p>Deputy Head of Library Services: Agreed. In the process of a restructure which is anticipated to be completed by the end of the year and the post of Systems Librarian will remain with the intention to have this post filled. The Deputy Head of Library Services is currently covering elements of the Systems Librarian role with support from HFBP. Library Services management will be investigating and negotiating with Civica for technical support which will require director permission.</p> | Deputy Head of Libraries (LBHF) | 01/12/2010 |

2. Enforced password changes and password complexity

| Priority | Issue | Risk | Recommendation |
|----------|---|---|---|
| 3 | <p>It was identified that access to the Spydus system requires that the staff user initially log on to the Council network which involves the use of a secure generic logon to the Customer Service Desk that has been formally approved by the business. A further unique user ID and four digit PIN code is required for access into Spydus and to perform activities, such as Cash Management; however, the system does not currently enforce the user to change their PIN on a periodic basis and PIN/password complexity requirements are not currently enforced.</p> <p>It is acknowledged that enforcing PIN rules and security parameters for password complexity, expiry and password history on the current version 8.5.1 of the Spydus system for staff would affect all users including the public customers.</p> | <p>Where the system does not enforce the user to change their PIN on a periodic basis and PIN/password complexity requirements are not enforced, unauthorised users may be able to access the system and compromise the data contained within the system.</p> | <p>The current access controls, in the form of a unique user ID and PIN control access into the Spydus system, should be evaluated, strengthened and enforced by the system. The following password controls should be considered for staff users:</p> <ul style="list-style-type: none"> • Passwords are force changed upon first logon; • Passwords are force changed on a periodic basis; and • A password history is maintained to prevent re-use. |

| Management Response | Responsible Officer | Deadline |
|---|---------------------------------|------------|
| <p>Systems Librarian: Agreed. The next release and upgrade of Spydus system will enable staff users to change their passwords.</p> <p>Deputy Head of Libraries: For the front line library staff, this will prove to be practically difficult to implement. Currently, access is to borrower information and not sensitive data, however, an assessment will be made if it is beneficial for the service.</p> | Deputy Head of Libraries (LBHF) | 01/10/2010 |

3. Lockout after unsuccessful login attempts

| Priority | Issue | Risk | Recommendation | |
|---|--|---|--|------------|
| 3 | The current version 8.5.1 of the Spydus Library Management System does not lock staff users out after unsuccessful login attempts. | Unauthorised users may gain access to the system through password guessing. If accounts automatically unlock after a pre-defined time period, then these unauthorised attempts may not be identified. | Consideration should be given to the Spydus Library Management System locking staff users out after a pre-defined number of unsuccessful logon attempts. In this event, only the System Administrator should be able to unlock the user's account after verifying the identity of the user. Furthermore, periodic monitoring and reporting of failed logins should be performed. | |
| Management Response | | | Responsible Officer | Deadline |
| <p>Systems Librarian: Agreed. This would be a request to Civica and responsibility for the Deputy Head of Libraries.</p> <p>Deputy Head of Libraries: Agreed. An assessment will be made if it is beneficial for the service.</p> | | | Deputy Head of Libraries (LBHF) | 01/10/2010 |

4. SLA for the Library service and Spydus system

| Priority | Issue | Risk | Recommendation |
|----------|---|---|---|
| 2 | <p>At the time of the audit review, a formal SLA between HFBP and the Library Services for the in-house support and maintenance of the services and systems including Spydus was in the process of being drafted for the business owner. Currently, support arrangement with its terms and conditions falls under the remit of the overarching SLA for systems and services across the Council and not a specific SLA for Library systems and services.</p> <p>Audit review identified that there were 37 issues outstanding for action, update and resolution for the Library Service with 17 incidents which were in relation to Spydus. With the Systems Librarian acting as the only designated Systems Administrator for Spydus and having left at the end of June 2010; it is essential that HFBP perform an assessment of System Administration support in this key absence and to help ensure continuous service and monitoring of incidents without exposure to significant disruption to the library service.</p> | <p>Without a specific SLA defined and documented for the Library Service and the Spydus system, with procedures established to monitor the IT services rendered by HFBP, there is an increased risk that the Spydus system may not be adequately supported which could result in the poor delivery of a library service by staff to the public.</p> | <p>The Council's partners for ICT managed services, Hammersmith & Fulham Bridge Partnership (HFBP) should perform a full evaluation of the systems and services provided to the Libraries, particularly in response to the Library Service having lost the Systems Librarian. Furthermore, to define and formally approve with the Library Service and implement a specific formal Service Level Agreement (SLA) with procedures established to monitor the service of in-house support and maintenance of the Spydus application and library services against the SLA.</p> |

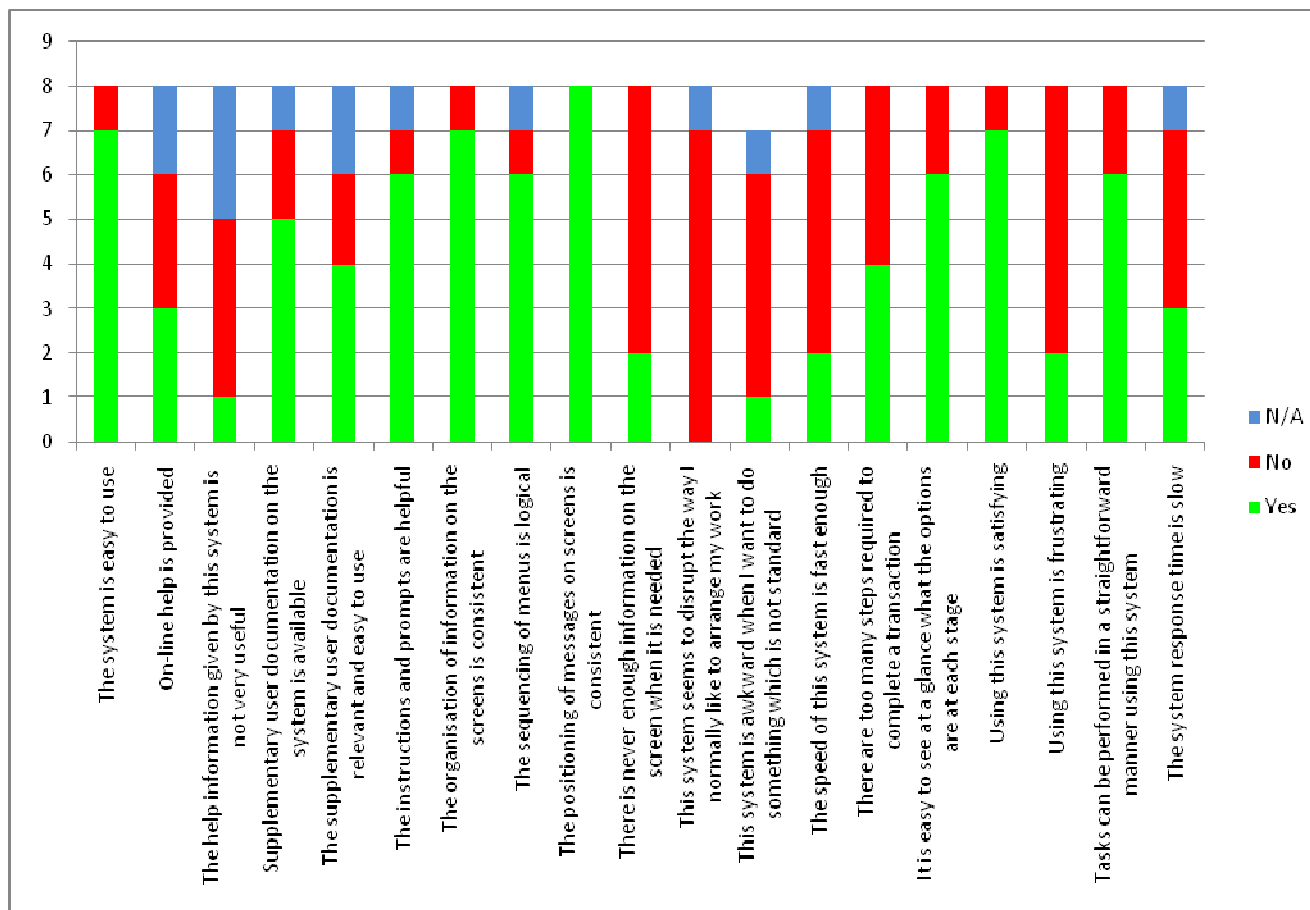
| Management Response | Responsible Officer | Deadline |
|--|---|------------|
| <p>Systems Librarian: Agreed. This would be directed for comment and action by the Deputy Head of Library Services.</p> <p>Head of Application Services and Application Support Analyst, HFBP: Agreed and a specific SLA for Library Services is in the process of development which requires review and approval by the business owner.</p> <p>Deputy Head of Libraries: Regular meetings are taking place with the Business Support Lead from HFBP for Spydus and resolving issues, discussing and submitting Work Package Requests (WPR).</p> | Deputy Head of Libraries (LBHF) and Head of Application Services (HFBP) | 01/03/2011 |

Appendix A – Results of Spydus Application Assessment Questionnaire

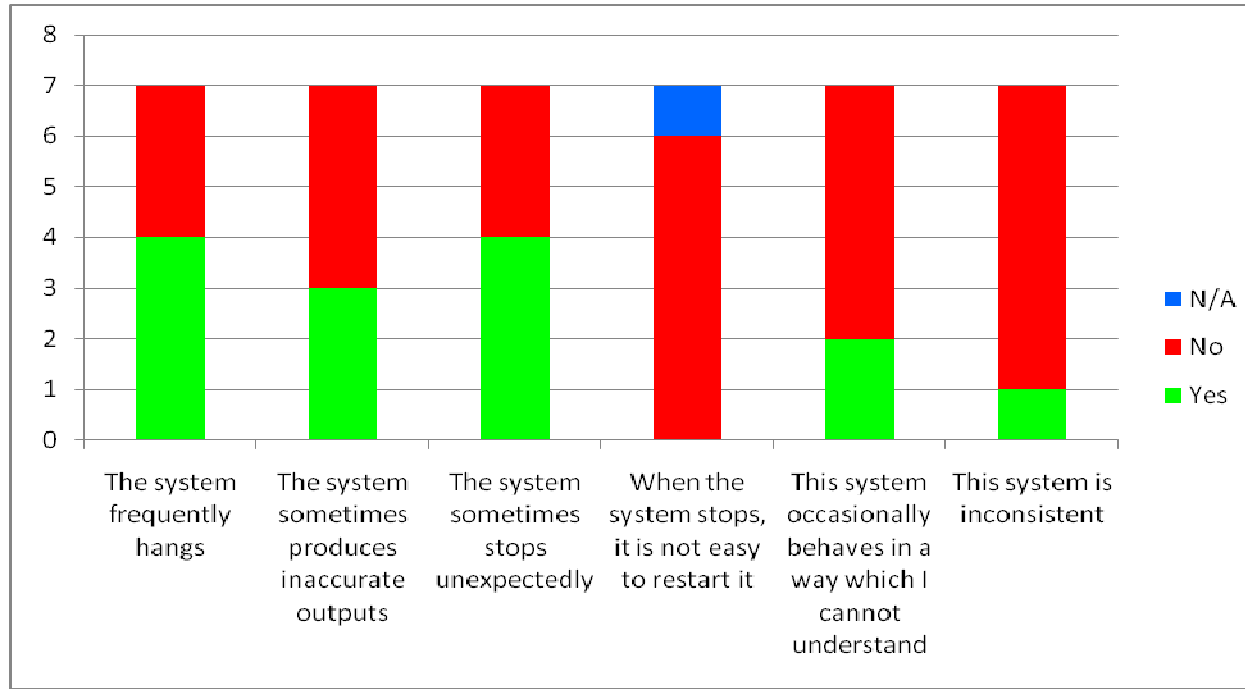
In addition to the application audit, we circulated a Spydus Application Assessment Questionnaire in order to capture the views of users on a number of areas in an attempt to establish any practical issues relating to the use of the system. The areas identified covered in the questionnaire were Usability; System Reliability; System Delivery of Required Outcomes, and System Failure.

A summary of the responses to the questionnaire have been illustrated in the tables below:

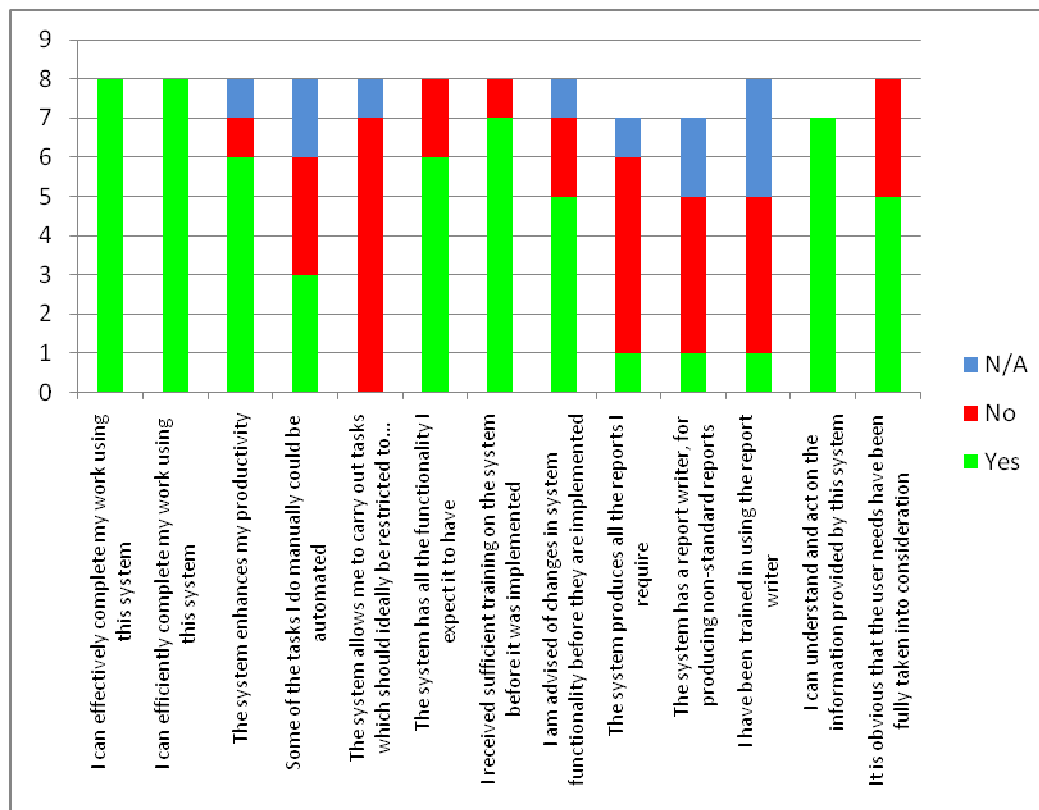
Usability



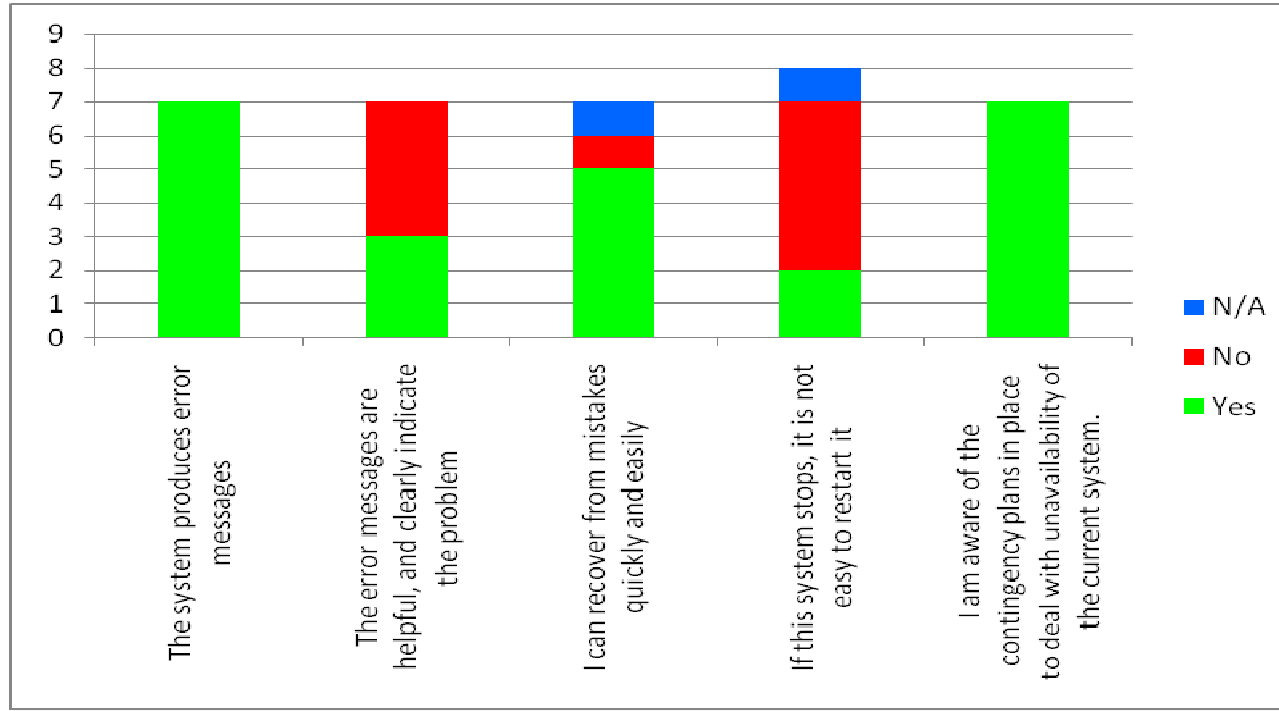
System Reliability



System Delivery of Required Outcomes



System Failure



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

June 2011

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

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, which is the United Kingdom member firm of Deloitte Touche Tohmatsu. Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

©2011 Deloitte & Touche Public Sector Internal Audit Limited. All rights reserved.

Deloitte & Touche Public Sector Internal Audit Limited is registered in England and Wales with registered number 4585162. Registered office: Hill House, 1 Little New Street, London EC4A 3T