INTERNAL AUDIT REPORT

FROM: Audit and Risk Manager

TO: Head of Finance
Principal Accountant (Capital and Treasury Management)
ICT Services Manager
ICT Infrastructure Manager
ICT Application Support Manager

C.C. Chief Executive
Head of Corporate and Community Services

SUBJECT: ICT Business Applications – Paris Income Management

DATE: 30 September 2012

---

1. INTRODUCTION

1.1. In accordance with the Audit Plan for 2012/13, an examination of the above subject area has been undertaken and this report is intended to present the findings and conclusions for information and action where appropriate.

1.2. My thanks are extended to all concerned for the help and co-operation received during the audit.

2. SCOPE AND OBJECTIVES OF AUDIT

2.1. The examination was undertaken to assess the adequacy of key controls in place for the Paris Income Management application to ensure the completeness, accuracy, security and effectiveness of data input, processing and output. These controls may be provided either by programming within the application system or by manual controls exercised by users or ICT Services.

2.2 The review focused upon the key IT application controls in place for the following areas:

- management of user access;
- role of system administration;
- data integrity;
- provision of audit trails;
- arrangements for application recovery;
- system development.

2.3 The audit approach used the Application Controls module of the CIPFA Matrices for Information Technology supplemented by adapted elements of the Change Control module. The expected controls under these Matrices are categorised into the following areas:

(1) Compliance
(2) Logical Security Controls

(3) User Security Controls
(4) Parameter Data
(5) Transaction Input
(6) Data Processing
(7) Output
(8) System Availability
(9) Audit Trail
(10) Change Control – Application Release.

2.4 The audit approach was to evaluate the controls by completion of an Internal Control Questionnaire and undertaking compliance tests applying the CIPFA Matrices model where appropriate. This was performed through:

- consultation and discussion with the system owner and persons responsible for system administration and technical support (from both ICT Services and the system supplier); and
- inspection and analysis of relevant documentation, system reports, displays, data exports, etc.

2.5 Recommendations from the previous audit of the Paris application were considered and status on management action ascertained.

3. AUDIT FINDINGS

3.1 Recommendations from Previous Report

The current status regarding the recommendations from the previous review undertaken in 2008 is as follows:

Recommendation	***Current Position***
The roles and responsibilities of the System Owner and system administrators should be formally documented, with designated individuals being notified. *(Low risk)*	*It was advised that a responsibilities document had been drawn up which system owners/administrators were required to sign up to.*
The use of a single sign-on authentication mechanism to the PARIS application, using the computer network operating system to authenticate authorised users, should be investigated. A project should be established to implement this functionality if it is deemed to bring benefits to the underlying business processes. (NB whilst this report relates specifically to PARIS, the use of a single sign-on mechanism could also be investigated for any other relevant systems). *(Low risk)*	*Some enquiries were made with the system support service. Single sign-on requires integration between the application and Windows Active Directory (part of the network operating system supporting management of resources and access to them). It was advised by the vendor that no plans to integrate were in place for the foreseeable future.* *It should be noted that single sign-on is not in place for any of the Council's main business applications.*

Recommendation	***Current Position***
The audit logging process (as advised by Anite) should be reviewed to ascertain whether it is feasible and would not adversely affect the performance of the system, with subsequent implementation as appropriate. *(Low risk)*	*Enquiries revealed that that a tool is available to monitor changes to parameters (the subject of the recommendation), but this does not appear to have been followed through. Support for the application has been taken over from Anite by Northgate who advised that a system release extending audit logging to include parameters would be available in late summer 2009. In the event release has not been installed. This issue is further discussed in 3.8 below.*
Testing should be undertaken (within the test environment) to ascertain if amendments to the clock / date settings on the workstation have an effect on the date that transactions are receipted. *(Low risk)*	*Status: It was advised that changes to the applicable group policy have been implemented to lock down the workstation time zone, date and time.*

3.2. Current Audit Findings

3.2.1 The PARIS application operates two main functions – cash receipting and electronic income transaction processing. Although the system also has internet and telephone payment processing capability, this is not implemented. There have been no system releases installed since the previous audit so system version remains in operation, although there a major upgrade is being explored with a view to implementation in the near future.

3.2.2 As stated above, Paris is now supported by Northgate although this does not affect the software license agreement which is with a separate agency under the government's Buying Solutions framework and combines Paris with the TOTAL financial management system.

3.3 Compliance

3.3.1 Appropriate regulatory controls were found to be in place to ensure that the application meets applicable statutory requirements and its use complies with relevant legislation and internal policies. The following key controls have been verified from testing:

- Applicable purposes of processing data have been notified as required under the Data Protection Act 1998;
- Appropriate system documentation is in evidence; and
- The system ownership provisions of the corporate Information Security and Conduct Policy have been observed for the application.

3.3.2 In its limited state of use, there is no legislation specific to the application which partly accounts for the infrequent take-up of system releases. Corporate management frameworks are in place for compliance with Data Protection and Freedom of Information legislation.

3.4. Logical Access Controls

3.4.1 Within the confines of the inherent design of the application, the logical security controls were found to substantially meet the following expected standards:

- assignment of unique user identifiers and passwords with access to create, change or disable users restricted to designated system administrators;
- parameters to enforce disciplines for user passwords available and set at an appropriately secure level;
- users are denied details of which login component is invalid in the event of a failed login attempt;
- limits to failed login attempts before user lock-out;
- user role structure enabling access permissions to be tailored to users' responsibilities;
- user profile data are tables protected including encryption of passwords;
- only modules and system functions allowed to users are displayed.

3.4.2 Review of access controls to the 'backend' database showed appropriate restrictions in place, subject to an observation regarding vendor access.

3.4.3 The Paris database runs on a server which also hosts the Total financial management database and each has a separate support contract under which the vendor is permitted to remotely access their own respective product. The current access configuration effectively gives the Total vendor full administration privileges over the Paris database for which they have no contracted support authority.

3.4.4 This is the result of system administration privileges being assigned at the higher SQL Server 'instance' level which applies to all databases running on that instance (in this case Total and Paris but no others).

Risk
Incorrect and unauthorised changes to the Paris database could be made by the Total vendor.

Recommendation

The ICT team should confirm why the vendor for Total is provided with SYSADMIN access at instance level. Steps should subsequently be made to ensure that the Paris database cannot be accessed by the Total vendor.

3.5 User Security Controls

3.5.1 Appropriate controls are in place to ensure that:

- operational users are made aware of their responsibilities when using the application (including a sign-up to the Information Security and Conduct Policy and on-line ICT induction; and

- access rights are promptly removed for operational users who leave the Council or change duties assisted by leaver reports from Finance (Payments).

3.5.2 An examination of current user, group and permission data did not reveal any issues.

3.6 Parameter Data

3.6.1 The examination showed the parameter data to be adequately protected with access restricted to a small core of responsible officers that are independent of those involved in day-to-day operational processes.

3.6.2 There is no requirement for periodic updating of any parameters. In practice the global system parameters are fixed and recognition rules for posting imported transaction data rarely change. Look-up tables for feeder system accounts are updated daily automatically.

3.5 Transaction Input and Data Processing

3.5.1 Processing controls for this application operate mainly at the input stage with two forms of input:

- 'Manual' input using the counter receipting module, mainly undertaken by the Document Management Centre, Reception and One-Stop Shops. This input is controlled via the use of drop-down lists, mandatory entries, fixed formats and matching to ledger code and feeder account references/balances (e.g. rent, council tax, debtor account, etc.).

- Daily imports from other, external, systems such as Allpay, internet and banking systems where input is controlled by the use of pre-set file structures and inbuilt validation routines. The import files are saved by Finance to specific network folders with restricted access and uploaded to PARIS using scheduled tasks which are validated and can be reported on using the Activity Log.

3.5.2 Not all the raw data from the daily imports is uploaded to Paris with source bank and debit/credit card account details in particular excluded. Unfortunately, some unique references are also left out inhibiting tracing of transactions (a known example of this is payments through the Planning Portal). In a discussion with the System Owner, it was advised that changes in file structures to accommodate additional fields from the source data will inevitably involve a significant cost that is not seen as warranted from the current limited scale of Planning Portal transactions.

3.5.3 In a test, the auditor (a Paris user with permissions restricted to view and report generation only) was able to access the 'working directory' using Windows navigation tools armed only with the server name. This included being able to access daily import files going back up to six years albeit on a view only basis. On the internet payment files names and addresses were in full view, although all payment card numbers have six characters starting from the seventh digit 'asterisked' out in case each and some other sensitive fields are encrypted.

3.5.4 It is also known that copies of the import files are saved to the more secure Finance network folders for occasional reference (e.g. to process refunds by BACS). The question arises as to whether:

- the import and upload transaction files in the Paris 'working directory' can and should be purged regularly
- the Paris 'working directory' can be locked down from viewing via Windows navigation tools.

Risk
Unauthorised persons may gain access to income transaction data.

Recommendations

(1) A procedure should be implemented (subject to feasibility review) for regular purging of income transaction import files in the Paris 'working directory'.

(2) The feasibility of locking down the income transaction import files in the Paris 'working directory' against access through Windows navigation tools should be investigated.

3.6 Output

3.6.1 The primary output from the PARIS application is in the form of electronic tables to be uploaded automatically daily to the TOTAL Ledger and applicable feeder systems with validation against ledger codes and feeder system account references as applicable. Failed postings are subject to suspense item investigation and clearance routines. Printing of output is minimal and performed on local printers for direct collection by the initiators.

3.6.2 The bulk of output reports and listings are saved as electronic files in secure structured Finance network folders thus helping to preserve ensuring completeness and confidentiality.

3.7 System Availability

3.7.1 System availability is assured by a combination of supplier support, under formal contractual arrangements, and centralised in-house database management and data back-up overseen by the ICT Infrastructure Team.

3.7.2 Business continuity management is directed by a corporate framework which is subject to separate audit review. At the time of the audit, a process is currently in place whereby the Service Areas are updating their respective Crisis Plans. The auditor was permitted to view the draft plans for Corporate and Community Services and Finance, neither of which specify the cash receipting and income processing functions among the 'critical tasks'.

3.7.3 The ICT disaster recovery arrangements categorise Finance systems overall as Class 2 with recovery objectives of 7 days and 31 days for loss of host service and loss of entire host building respectively. In the event of application loss on the server, cash receipting transactions can still be input to designated work stations in stand-alone mode.

3.8 Audit Trail

3.8.1 The purpose of an audit trail is to ensure that:

- sources of transactions or amendments to standing data are traceable;
- output data is verifiable;
- system interfaces can be reconciled to substantiate financial ledgers;
- the guilty party can be identified in the event of a fraud or irregularity.

3.8.2 Within PARIS, each transaction is assigned an audit number which is sequentially generated for each different workstation. The absence of logging of changes to parameter data (or other non-transactional data) within the system was raised as an issues in the previous audit.

3.8.3 At the time of the audit, the issue remained unresolved. Feedback from Northgate stated that a system release with parameter change logging incorporated would be available in late summer 2009. This release was never installed.

3.8.4 The key may now lie in the upgrade currently being considered, although it is not known for certain whether this incorporates automatic parameter change logging.

Risk
Incorrect parameter and standing data changes may compromise system operation.

Recommendations

(1) Enquiries should be made with Northgate as to whether the scope of audit logging in the version of Paris being considered for migration includes parameter changes.

(2) Logging and reporting of parameter changes should be implemented, either as part of the envisaged upgrade or installation of the applicable system release previously produced as appropriate.

3.9 Change Control – Application Release

3.9.1 As a third party supplied product, changes to programmes can only be implemented through accredited releases issued by the software 'owner' (now Northgate). The following standard controls over implementation of releases operate:

- installation to the server can only be performed by ICT Services;
- implementation follows a global change policy Application Release Procedure and an application-specific release checklist;
- all releases are first installed in a testing environment separate from the live processing environment
- implementation of system releases and resultant down-time are prominently notified to all staff via the Council's Intranet;
- lead 'users' undertake testing prior to live implementation; and
- a Software Acceptance Certificate has to be signed by the system owner before the software changes are release into the 'live' environment.

3.9.2 There have been no system releases installed for Paris since the previous audit and therefore no activity to test.

5. CONCLUSIONS

5.1 Resulting from the examination, we are able to give SUBSTANTIAL assurance of effective controls in place ensuring completeness, accuracy, security and effectiveness of data input, processing and output for the Paris database application.

5.2 There was one previous recommendation still to be fully addressed – logging of parameter changes which may tie in with a system upgrade currently being considered. New issues to emerge are:

- isolated observations on network and database management configuration which indicate some potential for inappropriate access to the Paris database, although the actual risk of this occurring is seen as generally low;

- the accessibility, presumably to all Paris users, of imported income transaction files going back several years via Windows navigation tools (although view-only access is possible in this manner, the risk of inappropriate access to personal data content should be considered).

6. MANAGEMENT ACTION

6.1 The recommendations arising are reproduced in the appended Action Plan for management response.

Richard Barr
Audit and Risk Manager