INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	PARIS Income Management
TO:	Head of Finance	**DATE:**	26 March 2018
C.C.	Chief Executive Deputy Chief Executive (AJ) ICT Services Manager Strategic Finance Manager Principal Accountant (Capital & Treasury Management) Principal Accountant (Systems) Systems Officer Portfolio Holder (Cllr Whiting)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2017/18 an audit review of the PARIS Income Management application has been completed. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 The PARIS application is used for cash receipting and to process and reconcile payments from multiple departments across the Council. This review of the system and its supporting controls was performed in order to provide assurance that there are no data security or application control weaknesses in the ICT security and management of the application.

3 Scope and Objectives of the Audit

3.1 The work included a review of application security, incorporating access rights and privileges, audit trails, system administration functions, application support, and data backup.

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

3.3 The audit was designed to assess and provide assurance on the following risks:

- Non-compliance with current policies and procedures
- Application availability / data integrity is impaired in the absence of sufficient application security controls
- Inappropriate accesses allowed to system functionality and / or data
- Users have access to data / information not applicable to roles and responsibilities
- Users are not removed when they leave, or access privileges are not changed when roles / jobs change
- High level and super user functions are not properly managed
- System and data backups are not properly carried out.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 The current position in respect of the recommendations from the audit reported in November 2012 is as follows:

Recommendation	Management Response	Current Status
1 The ICT team should confirm why the vendor for Total is provided with SYSADMIN access at instance level.	Remove sysadmin rights from TASK and warwickdc\consilium.	Completed.
2 A procedure should be implemented for regular purging of income transaction import files in the PARIS working directory.	The feasibility of the recommendation will be investigated and implemented if practical.	Due to staffing changes, management were unsure whether this had been actioned. The recommendation is, therefore, repeated in the action plan for this audit.
3 The feasibility of locking down the income transaction import files in the PARIS working directory against access through Windows navigation tools should be investigated.	Northgate have been consulted and they have been provided the necessary information. Application Support have started the required changes.	Completed – working directory files are no longer accessible through Windows.
4 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.	Northgate have been consulted. The audit logging of parameter changes in version 41 of PARIS.	Completed. Management have since upgraded to a newer version of PARIS.

Recommendation	Management Response	Current Status
5 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.	We will be upgrading to version 41 of PARIS as soon as possible.	Completed. Management have since upgraded to a newer version of PARIS.

4.2 Policies & Procedures

4.2.1 Key ICT policies and procedures relevant to application security, user administration and data backup and recovery were identified and obtained during the review. These were used in the process of reviewing the suitability of the controls in place for the PARIS application.

4.2.2 The policies identified as being of particular relevance in this review are the Information Security and Conduct Policy, Monitoring Policy, Software Policy and the Data Handling Policy.

4.3 Application Security

4.3.1 Authentication to the PARIS application is performed at the application level, with users being provided with password credentials that they are required to change on initial login.

4.3.2 It was found that strong passwords were enforced at the application level, as required by the Council's Information Security and Conduct Policy. Passwords are required to contain a capital alphanumeric character, a numeric character and a special character (such as @,$ or #). In addition the password itself must be a minimum of seven characters.

4.3.3 An audit trail of user activities is captured within the application, and reporting is available for review in the event of any suspect activity.

4.4 Access Control

4.4.1 It was noted that at the time of review ownership and responsibility for administration of the PARIS system was undergoing a period of change following the departure of the previous system owner, and that consequently there was a need to improve and / or formalise some of the supporting administration activities and controls.

4.4.2 Access to the application is currently provided by the Systems Officer, who has also recently been nominated the primary point of contact for support issues in relation to the system.

4.4.3 It was noted that requests for access to the application, or changes to existing users' access permissions, are made via a standard email rather than through the use of a user request form.

4.4.4 Rather than specifying the access individuals require in the system, or specifying a particular role based permission, managers generally nominate an existing member of staff to base the new starter's permissions on. It was also found that there is no explicit requirement that a record of user requests / changes to a user's access permissions is retained.

Risk

Users may have systems access not applicable to their roles and responsibilities.

Recommendation

Management should formalise the user request process via the use of a user request form, to be used when requesting new users or changes to existing users access permissions. Forms should be retained to provide assurance that appropriate access rights have been granted to users according to their job role.

4.5 **User Roles & Responsibilities**

4.5.1 Access permissions are assigned to users via the use of roles and groups within the PARIS application. It was noted that there are a large number of role profiles and groups but that there is no supporting documentation / notes clearly describing what access privileges within the application are assigned to each role / group.

Risk

Users may be assigned inappropriate access permissions.

Recommendation

Management should consider documenting the role profiles in order to gain better visibility of the access rights assigned to each role and provide further assurance that the correct level of access is being assigned to users.

4.5.2 Although accounts are reviewed on an ad-hoc basis, there is currently no regular exercise undertaken to review and verify that users' access levels within the application are appropriate i.e. that no users have been granted a high degree of access in error or that users have been able to retain and 'collect' access rights following a change of job role.

Risk

Users may be granted access permissions above and beyond that required by their job role.

Recommendation

A regular, at least annual, exercise should be undertaken to review users' access permissions within PARIS to ensure they remain appropriate.

4.6 Leavers Process

4.6.1 It is the responsibility of the leaver's team manager to notify ICT of leavers via the use of a leaver form, in order for a user's network and application accounts to be disabled. In the event that this form is not completed it is possible for accounts to remain active. It was found that the Systems Officer has additional controls in place to identify and remove leavers' accounts.

4.6.2 These controls include a process of comparing HR leaver data against live user accounts on a monthly basis and removing any leaver accounts identified, effectively mitigating the risks around leavers not being reported and removed from the system in a timely manner.

4.7 High Level & Superuser Functions

4.7.1 Administrator access rights, including the ability to create and delete users, are granted to a limited number of approved users. A list of the members of this group was obtained and reviewed with management during the review and it was confirmed that each user required this access and had the appropriate level of access for their job role.

4.7.2 A review of high privilege PARIS user accounts identified the existence of an active administrator level account named 'Administrator'. Although it is understood this account is unused and that ICT staff use named individual accounts for administration purposes it is possible the account could be used maliciously, or in error, to perform activities that cannot be easily traced back to an individual.

Risk

There may be a lack of accountability with the audit trail of actions performed showing the use of a generic administrator level account.

Recommendation

The purpose of the 'Administrator' account should be investigated and, if possible, the account should be renamed or deleted in order to remove the potential for misuse.

4.8 Database Security

4.8.1 Database security controls including authentication requirements, logging settings, and use of default / generic accounts were reviewed using the Microsoft Baseline Security Analyser (MBSA) tool, with scans of key PARIS servers performed and reviewed for potential security issues.

4.8.2 It was noted as part of this exercise that the SQL instance relating to the application uses 'Mixed Mode' authentication, rather than using Windows authentication (which would provide improved security). It was found that this is required by the application supplier as part of their support arrangements and that a change could have an adverse impact of the system operation and could not be easily altered. This has, therefore, been raised to highlight the security level but not as an issue to be resolved.

4.9 Backup & Recovery

4.9.1 Backups of the PARIS servers and database are made using HP Data Protector. Daily backups are made each night and kept in the onsite tape library for two weeks.

4.9.2 Backups are performed over the weekend and include all systems. The weekly tapes are taken by a member of the Infrastructure team to be stored off-site at the Town Hall where they are kept for a four week period. Monthly full backups are also made and taken off-site on a monthly basis. These are retained for six months.

4.9.3 It was found that, whilst regular backups are made and retained, there has been no testing of the ability to restore PARIS data from backups that management are aware of.

Risk

There may be limited or no assurance that the application can be recovered within an acceptable timescale and that potential issues have been identified and addressed.

Recommendation

Testing of PARIS should be scheduled as part of the next disaster recovery testing exercise. The testing should be documented and include the time taken to recover systems and services, whether recovery time and point objectives have been met and include detail on any issues and actions arising from the testing.

5 Conclusions

5.1 The audit identified three medium and three low rated recommendations, giving a MODERATE level of assurance around the application security of the PARIS application.

5.2 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 **Management Action**

6.1 The recommendations arising above, are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of the PARIS Income Management Application – March 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.1.1	A procedure should be implemented for regular purging of income transaction import files in the PARIS working directory.	Data may be retained longer than is necessary.	Low	Strategic Finance Manager / Principal Accountant (Capital & Treasury Management)	The feasibility of the recommendation will be investigated and implemented if practical.	September 2018
4.4.4	Management should formalise the user request process via the use of a user request form, to be used when requesting new users or changes to existing users access permissions. Forms should be retained to provide assurance that appropriate access rights have been granted to users according to their job role.	Users may have systems access not applicable to their roles and responsibilities.	Low	Strategic Finance Manager / Principal Accountant (Capital & Treasury Management)	This will be addressed, alongside recommendation 4.5.1. A user request form will be prepared to reflect the revised access levels. This will denote the appropriate access level, manager approval and system administrator verification that all documentation and training has been issued and performed.	August 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.5.1	Management should consider documenting the role profiles in order to gain better visibility of the access rights assigned to each role and provide further assurance that the correct level of access is being assigned to users.	Users may be granted inappropriate access permissions.	Low	Revenues Manager / Systems Administration Officer	This will be addressed in line with 4.4.4. The system needs to be streamlined. Currently the roles identify individual requirements and are not of a generic nature. It is the intention of Finance management to reduce the number of profiles to ensure correct access rights are allowed to applicants based upon job description. This ensures any changes required are applied to all users correctly with a reduction of system admin time to manage profiles within the system. The issue will be raised with the system supplier (Northgate) to ensure that changes to existing roles will not have any adverse effect.	August 2018
4.5.2	A regular, at least annual, exercise should be undertaken to review users' access permissions within PARIS to ensure they remain appropriate.	Users may be granted access permissions above and beyond that required by their job role.	Medium	Revenues Manager / Systems Administration Officer	To be done annually.	Annually in October

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.7.2	The purpose of the 'Administrator' account should be investigated and, if possible, the account should be renamed or deleted in order to remove the potential for misuse.	There may be a lack of accountability with the audit trail of actions performed showing the use of a generic administrator level account.	Medium	Revenues Manager/ Systems Administration Officer	To be suspended, alongside any other redundant generic user accounts. In line with Corporate IT policy, all users should have an individually assigned user name and password which must not be disclosed to any other individual either within the organisation or outside.	Completed
4.9.3	Testing of PARIS should be scheduled as part of the next disaster recovery testing exercise. The testing should be documented and include the time taken to recover systems and services, whether recovery time and point objectives have been met and include detail on any issues and actions arising from the testing.	There may be limited or no assurance that the application can be recovered within an acceptable timescale and that potential issues have been identified and addressed.	Medium	ICT Manager	The next formal disaster recovery (DR) test is not for another twelve months. However, each month a system is recovered to our in-house standalone test environment which mimics the DR test. Therefore, the PARIS system will be recovered to this environment as part of the April '18 test. As per standard practice a helpdesk job will be raised and all relevant recovery data will be logged within the job and shared with the System Owner.	April 2018

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.