Internal Audit Report

Finance

Financial Ledger System

Issued to:
Steven Whyte, Director of Resources
Jonathan Belford, Chief Officer – Finance
Fraser Bell, Chief Officer – Governance
Carol Smith, Accounting Manager
Graham Stubbins, Finance Manager (Systems)
External Audit

Date of Issue: February 2020 **Report No. AC2016**

EXECUTIVE SUMMARY

The Council uses the financial ledger system for the Council's budget and accounting requirements. The annual system support and maintenance cost for the system and related reporting tools for 2019/20 is approximately £152,000.

The objective of this audit was to provide assurance over system controls, business continuity and contingency plans. In general, this was found to be the case.

System performance is being adequately monitored and corrective action is being taken to improve performance where required. A contract is in place with the supplier which includes a Data Processing Agreement that complies with data protection legislation. Timetables covering relevant period and year-end accounting dates and requirements are available to staff. Reconciliations of the creditors and debtors sub-ledgers to the general ledger were taking place timeously and the suspense accounts, for transactions interfacing with the financial ledger with invalid or no financial codes, are being regularly reviewed and cleared. In addition, system disaster recovery testing has been scheduled to take place in 2020 in accordance with scheduled arrangements with the Council's data centre service provider.

System access controls were found to be adequate however a recommendation was agreed with Finance to ensure mandatory finance training is completed prior to access being granted to the system.

1. INTRODUCTION

1.1 The Council utilises the Advanced Business Software and Solutions Limited (ABS) eFinancials v5.0 financial ledger system for the Council's accounting requirements. The System is capable of reporting the Council's budgeted and actual financial position. A number of additional reporting tools are used in conjunction with eFinancials by budget holders and Finance staff, including Collaborative Planning, eAnalyser and SAP Business Objects.

1.2 The annual system support and maintenance cost for the system and relating reporting tools for 2019/20 is approximately £152,000.

1.3 The objective of this audit was to provide assurance over system controls, business continuity and contingency plans.

1.4 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Jonathan Belford, Chief Officer – Finance, Carol Smith, Accounting Manager, Graham Stubbins, Finance Manager (Systems), and Richard Burnett, Finance Controls Accountant.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Procedures and Training

2.1.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff, important in the event of an experienced employee being absent or leaving.

2.1.2 A variety of eFinancials user guides and interactive courses are available on the Zone and the Council's online interactive learning module, which include relevant system screen shots. User Administration procedures are available within a Finance network drive, covering administrative tasks, such as: how to reset a user password and amend user authority limits.

2.2 System Supply and Maintenance

2.2.1 An annual contract for support and maintenance has been in place for a number of years and one-off license fees are paid for upgrades and additional modules. This covers an unlimited number of users in relation to eFinancials, eAnalyser, Collaborative Planning and the web-based journal upload software Xcel uploader.

2.2.2 In accordance with the Council's Procurement Regulations, the Strategic Commissioning Committee were requested to approve a business case and procurement work plan relating to a contract extension from 1 December 2019 to 30 November 2024 for the above system and reporting tools. This was approved on the basis of the detail submitted to Committee.

2.2.3 The system is supported and maintained by the Finance Systems Team (FST), Digital and Technology (D&T), the system supplier and the Council's Data Centre provider. Issues affecting the application, its interfaces the databases or servers will, in the first instance, be raised with D&T via the ServiceNow portal. Where an issue cannot be resolved locally, and it relates to the servers, it is referred to the Data Centre provider, whilst those relating to the application, database and interfaces are raised with the supplier directly via the supplier's portal.

2.2.4 As at 8 November 2019, there were two active cases logged with the software supplier, both of which had been given the lowest priority rating of 4. Neither issue related to problems with the financial ledger.

2.2.5 The Finance Manager (Systems) advised that meetings were no longer taking place with D&T to discuss system performance issues. This increases the risk of the FST being unaware of ongoing system problems and developments, which could affect the administration of the system.

Recommendation
D&T should liaise with the FST regularly regarding system performance.

Service Response / Action
Agreed. D&T will set up key stakeholders' meetings which will include Service, Supplier and Digital & Technology representatives.

Implementation Date	Responsible Officer	Grading
April 2020	Digital Operations Manager	Important within audited area

2.2.6 The software supplier issues maintenance packs (patches) for system updates, containing instructions on how to carry out the maintenance activity. The maintenance packs are reviewed by the FST and applied by the FST where possible. Where this is not possible, D&T will be requested to apply the patch. Prior to patches being applied to the live system, they are tested by the System Owner. Software patches are recorded on a spreadsheet maintained by the FST, detailing when the patch was received, when it was tested, whether it resolved the problem and when the revised version of eFinancials went live.

2.2.7 In response to specific performance issues reported by the FST, the software supplier will produce an SQL (standardised query language, used for database management) to be applied to the system. Running an SQL will allow the system to be updated and resume normal functioning. The Service maintains a spreadsheet detailing a list of all SQLs that have been applied since 28 June 2018, their purpose, date and time applied, and the name of the system user who applied each. All entries were complete.

2.2.8 The last major system upgrade took place in June 2017 when the system switched to eFinancials 5.0 from 4.1 at a cost of £35,675. The next significant upgrade is scheduled for September 2020, when eFinancials 6.0 will be applied.

2.3 System Access

2.3.1 Access is granted to eFinancials by the FST on receipt of an authorised new user form, detailing the required access rights. Access rights of 'Enquiry', 'Input' and 'Training' are available for the eFinancials general ledger, and 'Enquiry' and 'Training' for eAnalyser. Access can be requested to be the same as an existing user. Where the access is unique, the financial codes which the user can have access to must be specified.

2.3.2 Authorised signatories requesting access to eFinancials are required to confirm the proposed user has completed "Data Protection – Essentials" and the "Corporate Data Protection" courses however these have been replaced with the mandatory online Information Governance course.

Recommendation
The new user form should be updated to reflect current training requirements.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
Implemented	Finance Controls Accountant	Important within audited area

2.3.3 Access levels can be amended or removed on receipt of an authorised 'Amendments to eFinancials / eAnalyser Access' form. Access levels can be added or removed for enquiry and input including in relation to financial codes. It is not currently possible to lock user access after a period of inactivity. Access rights are only revoked when the FST is notified to do so, or if the employee with access terminates their employment with the Council.

2.3.4 A unique user ID and a temporary password, which must be changed when the user first logs in, are provided by the FST. The Financial Ledger System password requirements are in accordance with the Council's ICT Access Control Policy and accompanying Password Standard.

2.3.5 Test and Train versions of eFinancials are available for testing software updates and training staff and these contain the same data as the live system up to the point at which

they were last refreshed. The systems are subject to the same password controls as the live system.

2.3.6 Access to the system is blocked after three incorrect password attempts; this was confirmed by Internal Audit. The system does not produce reports on multiple failed log-in attempts however the FST is required to be notified by the user by email for the user's password to be unlocked, and a temporary password, that has to be changed when first used, is emailed to the user.

2.3.7 The system automatically logs an audit trail of user activity which cannot be amended or deleted; however, this is not monitored. System Administrators (superusers) have the ability to disable the audit trail function; the Finance Manager (Systems) advised that this has never occurred before.

2.3.8 Administrative functions in relation to eFinancials are not monitored generally (in relation to the financial ledger), however purchase orders raised by System Administrators with superuser functionality are emailed to the Finance Controls Manager for monitoring purposes.

2.3.9 As at 4 December 2019 there were 636 users with access to the system. A sample of five New User Request Forms was selected to ensure each was completed and authorised and access was only granted if appropriate. Testing confirmed only two of the five employees were granted access to the system; the three denied access had not completed required training and in two cases had not indicated if they were aware of their responsibilities under relevant policies, including Financial Regulations. It was noted that one user granted access to the system had declared they were not aware of their responsibilities under Financial Regulations and had not completed the required course Finance Fundamentals.

Recommendation
Finance should ensure that all New User Request forms indicate required training has been completed and the potential system user is aware of their responsibilities under the relevant Council policies prior to access to the Financial Ledger System being granted.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
Implemented	Finance Controls Accountant	Significant within audited area

2.3.10 Monthly leaver reports sent by People and Organisation to the FST have temporarily ceased due to the implementation of a new payroll system. In the meantime, the FST has been identifying leavers as a result of undeliverable responses to monthly emails sent, via the generic ACC-Development email address, to staff in relation to general ledger, debtor and creditor closedown. Leavers are confirmed where emails cannot be delivered to the recipient. Leavers are also identified monthly by the FST using a HR system report of leavers. A sample of five leavers between April to December 2019 was selected from a list of leavers provided by Customer Experience, and it was noted that two former employee accounts had not been disabled, one of which related to an employee who left on 22 September 2019. Accounts of former employees should be closed timeously to reduce the risk of unauthorised access to the system.

2.3.11 The present system of identifying users who no longer require access to the system does not account for Council employees who have changed job within the Council and no longer

need access to the financial ledger system. An annual audit of user access would help to ensure user access remained appropriate and current.

Recommendation		
The Service should audit and update financial ledger system access, as required, regularly.		
Service Response / Action		
Agreed.		
Implementation Date	**Responsible Officer**	**Grading**
April 2020	Finance Manager (Systems)	Important within audited area

2.4 Data Protection

2.4.1 A Data Processing Agreement in the form of a contract addendum was signed by the system supplier and Finance in March 2018. As required by the Council's Corporate Information Handbook and the General Data Protection Regulation, this sets out the following:

- the subject matter and duration of processing;
- nature and purpose of the processing;
- type of personal information and categories of data subject;
- obligations and rights of the controller and the processor;
- security arrangement in respect of the processing.

2.5 Timetabling

2.5.1 Annual eFinancials timetables, detailing the creditor, debtor, purchase order and ledger period closure dates as well as the processing dates each period relate to, are published on the Zone. The timetable is maintained and updated by the FST with the current version updated on the 20 March 2019. This version includes closure dates up until the 28 February 2020.

2.5.2 Quarterly financial reporting key dates are made available through the Financial Monitoring timetable published on the Zone. A timetable had been included for 2019/20, detailing dates for budget holder, deadlines for Finance staff to update the ledger with accruals, and Committee reporting deadlines to the Chief Officer – Finance.

2.5.3 Comprehensive year end procedures have been posted on the Zone for the 2019/20 year-end. These include schedules for Services to return to Finance by 20 March 2020 which are required for the preparation of the Annual Accounts. Schedules include the year-end stock position and details of accruals and prepayments.

2.5.4 Finance has advised that they no longer maintain a rota for spreadsheet journal and interface processing since this is the responsibility of a single member of staff, however in the event this member of staff is absent it is the responsibility of the Finance Controls Accountant to complete these tasks.

2.6 Interfaces and Reconciliations

2.6.1 System interfaces update the ledger with creditors, debtors and general ledger journal transactions on a daily basis. Creditor interfaces include: the Payroll System; Consilium; Spydus; Clothing Grants; Education and Maintenance Allowances (EMA); Business Rates (NDR); ObCapture; Confirm; Estateman; and Tranman. Debtors interfaces include: Housing Advances; Trade Refuse; Housing Rents (IDOX); Xcel Uploader; and ICON Cash

Receipting. General ledger interfaces include: the Payroll System; ICON Cash Receipting; Xcel Uploader; BOXI; Collaborative Planning; and Housing.

2.6.2 Interface files run overnight and are posted to a CLINK holding area within eFinancials. The system has a number of automated checks which identify failures for Systems Analysts in D&T to take corrective action as required. Successful interfaces are sent by D&T to the Processing Team within the FST for posting to eFinancials, with details of the batch name, date, net amount, VAT, and number of transactions. In the case of creditor interfaces, system owners also send details of the interface batch, net amount, VAT and number of transactions. A reconciliation is then carried out by the Processing Team confirming the interface details, amount, and number of transactions per the clink file, per D&T, and per the System Owner (for creditors interfaces) agree. If these balance, the interfaces are posted to the ledger by the Processing Team.

2.6.3 Interfaces will commonly fail where a variance occurs, such as inputting a date out of the expected range for the period or an incorrect financial code. Duplicate interface uploads based on batch references and invoice numbers are also rejected by the system. Rejected transactions are automatically held in the CLINK holding area, with system generated exception reports produced as a result, detailing rejected transactions. The Processing Team reviews these reports and rejected transactions are queried with System Owners who are required to investigate the query and inform the Processing Team if rejected transactions should be processed or deleted.

2.6.4 A sample of 15 exception reports was selected from April to December 2019 to ensure System Owners had been notified of the rejections for investigation where required and appropriate corrective action was taken in a timely manner. Testing showed that corrective action had been taken for all exceptions and each correction was posted into eFinancials timeously. There were six instances where corrections were made by the FST in the absence of consultation with the respective System Owners. However, for each of these, minor / obvious reasons for failure were recorded and therefore resolved by the Processing Team to save time. However, there is not a standardised procedure in place detailing errors that the Processing Team can address in the absence of System Owner input. This increases the risk of inappropriate changes to financial coding of rejected transactions.

Recommendation
Finance should formalise interface processing carried out by the FST within a procedure including when System Owner input is not required to resolve interface errors.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
February 2020	Finance Controls Accountant	Important within audited area

2.6.5 As at 4 December 2019, the CLINK holding area contained no transactions that required to be cleared. A sample of 15 interfaces from April to December 2019 was selected to ensure that reconciliations were completed by the Processing Team and interfaces were posted in a timely manner. This was the case for the 15 interfaces reviewed.

2.6.6 At period end the debtors and creditors sub-ledgers are closed down and reports are run to confirm that this has taken place successfully. November and December 2019 debtors and creditors closedown reports were reviewed and the sub-ledgers had been closed in a timely manner. Following closedown of the debtors and creditors sub-ledgers, the general ledger is closed for the same period and a report is run to reconcile the respective general

ledger control accounts with the debtors and creditors sub-ledgers. The reports for November and December 2019 were both completed in a timely basis also and the general ledger debtor and creditors control accounts agreed to the respective sub-ledger balances.

2.7 Manual Data Input

2.7.1 Journals are used to make manual accounting adjustments in the financial ledger. On receipt of a journal voucher which is complete, balanced and adequately authorised, the Processing Team will post the journal, using Xcel uploader, which uploads spreadsheet journals. A journal description is required, as is the period, amount and financial coding. Journal references are automatically generated by the system when the journal is saved. Journals cannot be posted until mandatory fields have been completed and the debits and credits balance.

2.7.2 Journal upload is limited to 10 users based in Finance. The preparer and authoriser of a journal must be separate with the authority to approve journals as follows:

- Assistant Accountants up to £100,000
- Finance Development Officers up to 500,000
- Accountants – up to £2,500,000
- Finance Partners / Finance Operations Manager – unlimited

2.7.3 The Finance Ledger Journal Entry Procedure has been updated to reflect the above requirements and is accessible through the FST's shared drive. It was noted that an outdated Journal Input Manual is accessible on the Zone; this is no longer required since staff outwith Finance are no longer required to process journals.

Recommendation
The Journal Input Manual on the Zone should be removed.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
Implemented	Finance Manager (Systems)	Important within audited area

2.7.4 The period a journal should be posted to is recorded on the journal voucher sent to the Processing Team. All requests to backpost must be authorised by the Senior Accountant before they are referred to the FST, who will then review journals and determine whether it is reasonable to backpost.

2.7.5 A sample of 30 journals was selected between April and December 2019. These were checked to ensure that they were properly authorised, there was segregation of duties between preparer and authoriser, supporting documentation was present and the journals were input timeously and accurately by the FST. This was the case for all 30 journals reviewed, with the exception of one journal with a control value of approximately £2.9 million, authorised by a Senior Development Officer, despite the Financial Ledger Journal Entry Procedure stating Finance Development Officers only have authority to authorise journals up to a limit of £500,000, with journals over £2.5 million being the responsibility of Finance Partners and the Finance Operations Manager.

Recommendation
Finance should ensure journal authorisation is granted by the appropriate members of staff.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
Implemented	Finance Controls Accountant	Important within audited area

2.8 Suspense

2.8.1 Payroll and cash receipting system journals posted with invalid financial codes result in the associated transactions being posted automatically in eFinancials to the respective suspense account. The accounts are being regularly reviewed by the FST who receive email notifications every Monday and Wednesday in the form of a BOXI report of the suspense account balances. As at 14 January 2020 the suspense account codes all had a balance of nil.

2.9 Business Continuity and Disaster Recovery

2.9.1 The Council's Business Continuity Policy states that all Services must develop, implement and maintain Business Continuity Plans, that are to be reviewed and tested annually to ensure that:

- All critical functions are identified;
- The impact of the loss or disruption to these functions is identified and recorded; and
- Arrangements are in place to ensure the continuance of these critical functions at a predefined level in the event of an emergency.

2.9.2 The Finance Business Continuity Plan (version 6) was last updated in January 2019. Section 1.3 of the Plan defines a critical function of Finance as "maintenance of books and records in relation to financial transactions". E-financials is used for this purpose and is defined in section 1.8 of the Plan as being "difficult to replace". However, section 3.2.2 of the Plan, covering how critical functions will continue if key systems are lost, does not explain the process should access to e-Financials be lost.

Recommendation
The Finance Business Continuity Plan should be updated to cover the procedure should access to the Financial Ledger System be lost.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
March 2020	Accountant	Important within audited area

2.9.3 The business-critical systems, including eFinancials, are backed up in full on a weekly basis and incrementally on a daily basis by the Council's Data Centre provider. Thirty days of backup files are held locally with ninety-days of backup files held offsite.

2.9.4 The Incident and Problem Co-ordinator carries out disaster recovery testing in conjunction with the Data Centre Provider on agreed dates. A schedule of systems to be tested in the

next 4 years has been set up with testing dates included where known. eFinancials is included as one of the systems due to be tested and the Incident and Problem Co-ordinator confirmed this will take place during quarter 4 of calendar year 2020.

AUDITORS: D Hughes
A Johnston
C Jamieson

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the organisation.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.