ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	8 May 2018
REPORT TITLE	Internal Audit Report AC1812 – Financial Ledger
REPORT NUMBER	IA/AC1812
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on the Financial Ledger.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of the Financial Ledger.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or

Place, or Enabling Technology, or on the Design Principles of the Target Operating Module.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC1712 – Financial Ledger.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

BON ACCORD

ABERDEEN
CITY COUNCIL

Internal Audit Report

Finance

Financial Ledger System

Issued to:
Steven Whyte, Director of Resources
Sandra Buthlay, Interim Chief Officer - Finance
Fraser Bell, Chief Officer - Governance
Carol Smith, Accounting Manager
Graham Stubbins, Finance Manager (Systems)
External Audit

Date of Issue: March 2018 **Report No. AC1812**

EXECUTIVE SUMMARY

The Council utilises its financial ledger system for the Council's budget and accounting requirements. The annual system support and maintenance cost for the system is £90,000.

The objective of this audit was to consider whether appropriate control is being exercised over the system and that interfaces to and from other systems are accurate and properly controlled. In general, this was found to be the case, however recommendations have been made and agreed in relation to procurement; system access; data protection; timetabling; and, manual data input to the system.

1. INTRODUCTION

1.1 The Council utilises the Advanced Business Software and Solutions Limited (ABS) eFinancials v 5.0 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. Collaborative Planning is also used for budgeting and forecasting.

1.2 The annual system support and maintenance cost for eFinancials for 2017/18 is £90,000.

1.3 The objective of this audit was to consider whether appropriate control is being exercised over the system and that interfaces to and from other systems are accurate and properly controlled.

1.4 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Carol Smith, Accounting Manager and Graham Stubbins, Finance Manager (Systems).

2. FINDINGS AND RECOMMENDATIONS

2.1 Written procedures and Training

2.1.1 Comprehensive and clear written procedures are available on the Zone on the use of eFinancials. These cover a number of areas including: screen navigation; financial codes; general ledger enquiries; journal input and journal reversals. Clear written procedures are also available on the use of eAnalyser, Business Objects and Collaborative Planning.

2.1.2 An online course on the use of eFinancials and eAnalyser is available on the Zone. The course is interactive, includes relevant screen shots and requires the user to correctly answer questions before progressing.

2.1.3 User Administration procedures are available within the eFinancials application on: adding an eAnalyser licence to a user profile; adding access rights to a role; adding a cost centre to a user profile, user session tracking, confirming and amending a user authority limit and how to reset a user password. Written procedures are also available within the Finance Systems Team (FST) on how to process interfaces.

2.2 System Supply and Maintenance

2.2.1 A software license, maintenance and support agreement was made between the Council and the supplier in November 1998, with a license for 150 users to use eFinancials. The agreement remains in force until terminated in writing by either party and has been amended three times since introduction.

2.2.2 In October 2006, professional services were procured from the supplier to implement the reporting tool software, Collaborative Planning. In August 2007, a contract change made eFinancials, eAnalyser, Collborative Planning and the web based journal upload software Xcel uploader available to unlimited Council users through a new license, at a cost of £117,000. A further contract change agreement was subsequently made in March 2012 by the supplier granting the following SAP Business Objects licenses at a cost of approximately £119,000, including installation:

Software	Licences
SAP Business Objects Enterprise professional for Query, Reporting, Analysis (User)	220 Named Users
Business Objects Webi	40 Named Users
Xcelsius Enterprise Interactive Viewing (User)	10 Named Users
SAP Business Objects Xcelsius Enterprise (Designer)	1 Named User

The FST maintains a list of staff using Business Objects licenses for monitoring purposes.

The 2012 Contract Change Agreement has not been signed by the Council nor by the supplier. This increases the risk of contractual disputes.

Recommendation
The Contract Change Agreement should be signed by the Council and the supplier of the financial ledger system.

Service Response / Action
Agreed.

Implementation Date	**Responsible Officer**	**Grading**
March 2018	Finance Manager (Systems)	Significant within audited area

2.2.3 The Procurement Reform (Scotland) Act 2014 requires contracting authorities to maintain a register of regulated procurements detailing the date of award; name of the contractor; the subject matter; the estimated value; the start date; the end date; and the duration the contract can be extended. The support and maintenance contract for the Financial Ledger System is absent from the Council's contract register.

Recommendation
The Contract Register should be updated to include the details of the Financial Ledger System support and maintenance contract.

Service Response / Action
Agreed.

Implementation Date	**Responsible Officer**	**Grading**
May 2018	Category Manager	Significant within audited area

2.2.4 The supplier of the financial ledger system has remained unchanged for approximately 19 years, on a rolling annually renewed contract. The annual support and maintenance cost of eFinancials is £90,000. The Council's Financial Regulations state it is a statutory duty for the Council to obtain best value and that all purchasing must comply with the Council's Procurement Regulations. Procurement Regulations and The Procurement (Scotland) Regulations 2016 require procurements over £50,000 to be adequately advertised to ensure open competition. The Council's Procurement Regulations also require procurements over £50,000 to be approved by Committee prior to being undertaken.

2.2.5 Finance took part in a recent "soft review" of financial ledger system availability and concluded that the system currently in use continues to provide the necessary functionality. However, it is important to demonstrate continuing value for money and, in this regard, the Service should consult with Commercial and Procurement Services to determine the best way of doing so and of complying with procurement legislation.

Recommendation
The Service should consult with Commercial and Procurement Services to ensure that best value can be demonstrated in continuing with the current system and that procurement legislation is complied with

Service Response / Action
Agreed.

Implementation Date	**Responsible Officer**	**Grading**
June 2018	Finance Manager (Systems)	Significant within audited area

2.2.6 Support for eFinancials is provided by the FST, IT, the software supplier, and the Council's Data Centre provider. Problems affecting the application, its interfaces, the databases or servers are referred, in the first instance, to IT. Where an issue cannot be resolved locally and 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 software supplier. Details relating to open and closed support calls can be viewed on the supplier portal.

2.2.7 The Finance Manager stated that problems were experienced closing the Debtors system for period 8 with the process that began on 30 November not being complete until 2 December 2017. This problem has occurred previously and a call has been raised with the software supplier to investigate.

2.2.8 The FST receives weekly reports from ICT on the status of open eFinancials calls and details of those that have been closed in the previous week. One high priority call classed as 'awaiting user information' was raised in October 2016. This related to automating the process for transferring files for BACS transmission. The Finance Manager (Systems) advised that there used to be regular meetings with IT to discuss system performance issues such as these. The meetings have ceased meaning there is less awareness by the FST of how calls are progressing with IT.

Recommendation
Consideration should be given to reinstating meetings with IT to discuss system performance issues.

Service Response / Action
Agreed. A lift and shift review and planning meeting is to be held with IT and system owners. This will be considered at this meeting.

Implementation Date	**Responsible Officer**	**Grading**
February 2018	Finance Manager (Systems)	Important within audited area

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

2.2.10 The last system upgrade was in June 2017. The software supplier upgraded eFinancials to version 5.0 from version 4.1 at a cost of £35,675. IT assisted with this process by preparing servers, installing software, exporting data from the original database ready to be imported into the upgraded database and setting up database backups.

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. The financial codes which the user can have access to must also be specified.

2.3.2 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 as well as financial codes. Users who have left the Council are required to be notified to the FST using the form so that access to the financial system can be removed. It is not possible for the system to automatically remove access rights after a defined period of inactivity.

2.3.3 It is important that users are granted access to the financial system commensurate with their role, whilst simultaneously giving due consideration to segregation of duties. Guidance is unavailable to Third Tier Managers approving forms on what constitutes appropriate access for the purposes of authorising access forms.

Recommendation
Guidance should be made available to authorised signatories on what constitutes appropriate access to the financial ledger.

Service Response / Action
New user forms for eFinancials, PECOS and ICON are to be consolidated with choice of access for users being removed from the forms. The new form will require a description of why access to the system is required and the person's post details so that the FST can determine the appropriate access to be granted.

Implementation Date	**Responsible Officer**	**Grading**
April 2018	Finance Manager (Systems)	Important within audited area

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 Council's ICT Acceptable Use Policy requires passwords used to protect systems and applications to be maintained securely and comply with current guidelines. The Corporate Information Management procedure requires passwords to be at least 8 characters long and contain a mixture of numbers, letters and special characters. eFinancials only requires a minimum of 6 characters and there is no requirement for a mixture of numbers, letters and special characters. Ensuring longer, complex passwords enhances the security over system access.

Recommendation
The Service should amend system password requirements in line with the Corporate Information Management procedure.

Service Response / Action
Agreed. Password requirements have been updated within eFinancials in line with the Corporate Information Management procedure.

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

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 eFinancials is blocked after 3 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 the user cannot amend or delete, however these logs are not monitored or reviewed. There are 7 superusers of eFinancials within the FST, who can add and amend access to the system. Superuser activities are not currently monitored or reported. This increases the risk of fraud and error.

Recommendation
Superuser activity should be regularly reviewed by a Finance officer outwith the Finance Systems team.

Service Response / Action
Agreed. The FST will investigate if an automated monthly BOXI report of superuser activity can be set up and sent to the Accounting Manager for review.

Implementation Date	**Responsible Officer**	**Grading**
April 2018	Finance Manager (Systems)	Significant within audited area

2.3.8 As at 15 December 2017 there were 680 active users on eFinancials. A sample of 5 new users since April 2017 was selected and each was supported by an authorised form and access rights were considered appropriate.

2.3.9 The FST receive reports of leavers from HR on a monthly basis and remove access to the system for any users who have left the Council. There were 7 eFinancials users who left the Council in October 2017. As at the 15 December 2017 the user account of 1 of these leavers was still active, increasing the risk of unauthorised access to the system.

Recommendation
Leavers’ access to eFinancials should be deleted timeously.

Service Response / Action
Agreed. The FST has not been receiving leaver reports from HR recently. The Finance Manager (Systems) will investigate whether this can be reinstated for the purpose of removing leavers.

Implementation Date	**Responsible Officer**	**Grading**
May 2018	Finance Manager (Systems)	Important within audited area

2.4 Data Protection

2.4.1 The Council’s Data Protection Policy requires all staff who process personal information to undertake specified Data Protection Training at the commencement of their employment and also to complete regular refresher training thereafter. The financial ledger system includes personal information including payroll details of employees and therefore staff with access to the system should be aware of how such confidential data is required to be treated to avoid financial penalties and reputational damage resulting from any inappropriate use or loss of data.

2.4.2 The Council has three Data Protection related training courses: ‘Data Protection – Essentials’, which focusses on Data Protection, the employee Induction, which covers core Council policies for new employees and ‘For Your Eyes Only’, focussed on Information Security.

2.4.3 A sample of 25 employees who have access to eFinancials was selected to ensure they have completed Data Protection Training:

- 6 employees in the sample have not completed Data Protection Essential Training or For Your Eyes Only Training.

- 3 employees have not completed refresher training since 2012 and 1 employee has not done so since 2013.

Recommendation
Data Protection training should be completed by all staff with access to the financial ledger system in line with the Council's Data Protection Policy.

Service Response / Action
Agreed. The new access form will seek confirmation that Data Protection has been completed before access is granted to the financial ledger system.

Implementation Date	**Responsible Officer**	**Grading**
July 2018	Finance Manager (Systems)	Significant within audited area

2.4.4 The software licence, maintenance and support agreement signed by the software supplier in November 1998 includes a Data Confidentiality agreement. This states that if, during servicing or upgrading the software, it becomes necessary to access the Council's data, the supplier undertakes to ensure that the data will not be conveyed or transmitted in any form, to any other person or organisation other than the duly authorised representative of the supplier, and that data will be treated as strictly confidential. This provides contractual assurance that software supplier staff will manage Council data appropriately.

2.5 Timetabling

2.5.1 Annual eFinancials timetables which detail 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 last updated on the 13 December 2017. This version included closure dates up to the 28 February 2018.

2.5.2 Budget monitoring key dates are made available through the Financial Monitoring timetable published on the Zone. These include dates for budget holders to have updated Collaborative Planning with their most recent forecasts, deadlines for finance staff to update the ledger with accruals and prepayments, and reporting deadlines to Corporate Accounting, the Head of Finance, Service Management Teams and Corporate Management Team (CMT). The last timetable available is for 2016/17. This increases the risk that budget holders and Finance staff will be unaware of deadlines required to update the financial ledger.

Recommendation
A 2017/18 Financial Monitoring Timetable should be created and posted to the zone.

Service Response / Action
Agreed.

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

2.5.3 Comprehensive year end procedures have been posted on the Zone for the 2017/18 year end, which include schedules for Services to return to Finance by 23 March 2018, 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 The FST does not have a timetable or a rota for tasks carried out by the team. This increases the risk that team members will be unable to carry out all key tasks to gain experience and also increases the risk that tasks will be omitted in error.

Recommendation

A rota should be established within the FST, detailing deadlines for tasks completed by the team, responsible officers, and the date tasks have been completed.

Service Response / Action

Agreed. A review of FST duties is currently underway as part of the Target Operating Model. Responsibilities for FST tasks will be documented as a result of this process.

Implementation Date	**Responsible Officer**	**Grading**
May 2018	Finance Manager (Systems)	Important within audited area

2.6 Interfaces and Reconciliations

2.6.1 System interfaces update the ledger with creditors, debtors and general ledger journal transactions. Creditor interfaces include: the payroll system, the Social Work case management system; the Education Maintenance Allowance and clothing grant databases; and the non-housing repairs system. Debtor interfaces include: the cash receipting system and the housing rents; music fees; hanging baskets; and property factoring systems. General ledger journal interfaces include journals uploaded via Xcel journal uploader; cash e-Returns and 'K-Batchs' which include Council Tax and Business Rates journals.

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 IT to take corrective action as required. Successful interfaces are sent to the Processing Team by IT 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 ICT 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 Duplicate interface uploads are recognised by eFinancials based on batch references and invoice numbers and are automatically rejected, with rejected transactions held in the CLINK holding area. System generated exception reports are produced for the batches containing 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 deleted or processed. Exception reports for low value VAT differences will not be queried with System Owners and instead be corrected by the FST. A sample of 10 exception reports was selected from April to December 2017 to ensure System Owners had been notified of the rejections for investigation where required. This was found to be the case and transactions were posted after making the necessary corrections or deleted as appropriate by the FST. As at 26 January 2018, the CLINK holding area contained no transactions that required to be cleared.

2.6.4 A sample of 15 interfaces from May to January 2018 was selected to ensure that reconciliations were completed by the Processing Team and posted in a timely manner. This was found to be the case.

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. A Journal Input manual is available on the Zone, providing clear instructions with screenshots on how to post a journal in eFinancials. 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. Whilst the instructions are clear, they were produced in May 2008 and do not describe the responsible officers for preparing, authorising and posting journals.

Recommendation
The Journal Input Manual should be updated to include details of the responsible officers for preparing, authorising and posting journals.

Service Response / Action
Agreed. The Journal Input manual is out of date and will be removed from the Zone. The current journal procedure will be documented including responsible officers.

Implementation Date	**Responsible Officer**	**Grading**
May 2018	Finance Manager (Systems)	Important within audited area

2.7.2 A sample of 30 journals was selected from between 31 March 2017 and 20 December 2017. 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.

2.7.3 Two payroll journals were prepared and authorised by the same person. It was also noted that financial code corrections were required for two journals due to approved journals including invalid financial codes. The subsequent amended journals were not authorised before being posted.

Recommendation
All journals should be approved by an authorised signatory.

Service Response / Action
Agreed. An instruction will be issued to payroll staff.

Implementation Date	**Responsible Officer**	**Grading**
April 2018	Finance Manager (Systems)	Significant 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. Requests to post journals to closed ledger periods are referred to the FST who review the journal and determine whether it is reasonable to backpost it. There is no procedure for determining whether journals should be backposted.

Recommendation
A procedure should be prepared of acceptable reasons for re-opening closed ledger periods and shared with Finance staff.

Service Response / Action
Agreed.

Implementation Date	**Responsible Officer**	**Grading**
April 2018	Finance Manager (Systems)	Important within audited area

2.8 Suspense

2.8.1 Journals posted with invalid financial codes results in the associated transaction being posted automatically in eFinancials to a suspense account. The FST monitors this suspense account, sending details to the journal authoriser, to provide the appropriate correcting financial code. The suspense code transaction detail since 1 April 2017 was reviewed and it was confirmed transactions were regularly being cleared by the FST. The suspense code balance as at 16 February 2017 was nil.

2.9 Business Continuity and Disaster Recovery

2.9.1 The Council's Business Continuity Policy requires each Service to develop, implement and maintain Business Continuity Plans to ensure that: all critical functions are identified; the impact of the loss or disruption of these functions is understood and recorded; and arrangements are in place to ensure the continuance of critical functions at a predefined level in the event of emergency. Each Service must ensure these Plans are reviewed and tested at least annually.

2.9.2 The Finance Service Business Continuity Plan was last tested in October 2017, whilst the current version was prepared in December 2017. This describes eFinancials as a system which would be difficult to replace and the supplier as a Key Supplier. Services are required to obtain completed Key Supplier Assessment Questionnaires, to determine the adequacy of the Key Supplier's business continuity arrangements. Key Supplier Assessment Questionnaires were identified as being absent for all Key Suppliers in report AC1804 Business Continuity Planning in which a recommendation was made to update Procurement Guidance Notes to highlight the requirement for these questionnaires.

2.9.3 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 a ninety day backup held offsite.

2.9.4 eFinancials is maintained on Oracle version 12 databases. Transactions are backed up to the Oracle archive log continuously and each night the database and the day's archived logs are backed up to the Storage Area Network (SAN) at the Council's Data Centre provider. The Data Centre has configured the eFinancials Servers to have 'Snapshots' taken at intervals of less than a minute which can be used to rebuild a replica of the server.

2.9.5 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 however a date has yet to be agreed with the Council's Data Centre provider. A recommendation to schedule disaster recover testing has already been included in report AC1810 Major IT Business Systems.

AUDITORS: D Hughes
A Johnston
A Einoryte

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 Council.
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.