ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	8 May 2018
REPORT TITLE	Internal Audit Report AC1820 – PECOS
REPORT NUMBER	IA/AC1820
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 PECOS System.

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 PECOS System.

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 AC1720 – PECOS.

10.   REPORT AUTHOR DETAILS

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

Internal Audit Report

Finance

Professional Electronic Commerce Online System (PECOS)

EXECUTIVE SUMMARY

The Council utilises the Scottish Government's cloud based 'purchase to pay' Professional Electronic Commerce Online System (PECOS) system, to request, order and receipt goods and services, through a workflow based approval process. When requisitions are approved and orders raised, suppliers are notified via email. Between April 2017 and January 2018, 44,420 orders were placed by the Council using the system with a value of £57.379 million.

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 supply and maintenance; system access; user testing; data protection and business continuity planning.

The Finance Manager confirmed that results of testing are not fully documented prior to implementing system updates and upgrades. This increases the risk that system changes will not have been adequately tested resulting in unintended disruption to service users. It was recommended that the Service introduce a testing checklist for completion and approval prior to changes being implemented. The Service has advised that they do not have the resources available to test all PECOS updates. however they do make sure basic functions work prior to applying updates and upgrades and will document this in future.

1. INTRODUCTION

1.1 The Council utilises the Scottish Government's cloud based 'purchase to pay' Professional Electronic Commerce Online System (PECOS) system, to request, order and receipt supplies and services. Between 1 April 2017 and 31 January 2018, 44,420 orders were placed by the Council using the system with a value of £57.379 million. A monthly breakdown is as follows:

Month	Orders	Order Lines	Value £
April	3,780	21,843	5,765,494
May	5,751	36,772	6,414,216
June	5,399	35,292	5,696,249
July	1,985	10,349	5,671,420
August	3,511	23,037	5,461,479
September	5,005	31,494	3,887,131
October	3,833	23,642	4,015,878
November	5,907	38,362	5,360,086
December	4,220	27,896	6,703,060
January	5,029	32,889	8,403,582
	44,420	281,576	57,378,595

1.2 PECOS enables requisitions, purchase orders, order changes and the receipt of goods and services to be made electronically through a workflow approval process. When requisitions are approved and orders raised, suppliers are notified via email.

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, Corporate Governance.

2.   FINDINGS AND RECOMMENDATIONS

2.1   Written Procedures

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 of correct and consistent practices being followed, especially in the event of an experienced employee being absent or leaving.

2.1.2   As well as an on-line learning course on PECOS, there are a number of user guides available which can be accessed through the Zone. These cover all areas from setting up suppliers, requisitioning through approval to receiving of the goods / services. The manuals also include requesting access to the system and notifications when staff leave.

2.1.3   There are also a wide range of system administrator manuals and guides, covering all aspects of the system, available within the Finance Systems network folders. These provide detailed notes along with screen shots.

2.2   System Supply & Maintenance

2.2.1   PECOS is hosted by the developer on behalf of the Scottish Government and is available to the Council and other public sector bodies under the Scottish Government's eCommerce shared service Software License Agreement, free of charge. The Scottish Government has software license agreements in place with the developer and an IT professional services supplier for its support. A software license agreement must be signed by the Council to allow access to PECOS.

2.2.2   Annual support and maintenance is provided to the Council by a data centre provider, who download the Council's PECOS files from the developer's hosted site and convert these to the necessary format ready for uploading into the Council's eFinancials ledger system by that system's supplier.

2.2.3   The current data centre supply and maintenance contract, which expires in November 2018, costs £5,000 per annum and was procured through a Scotland Excel Support and Maintenance Framework. The annual interface contract with the Council's eFinancials supplier costs £8,200 and expires in March 2018.

2.2.4   The Council has a corporate license for PECOS with no limit on the number of users. A reporting package accompanies the system although only three licenses are provided free of charge. Two are held by the Finance Systems team and the other by Commercial & Procurement Services (C&PS). The Council should hold a copy of the software license agreement for the use of PECOS however a copy could not be located by C&PS or Finance.

Recommendation
A copy of the software license agreement should be obtained from the Scottish Government.

Service Response / Action
Agreed. This can be requested, but implementation will be dependent on the Scottish Government response.

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

2.3 **System Access**

2.3.1 Access is granted to PECOS by the Finance Systems Team (FST) on receiving a new user form, available on the Zone. A new requisitioner must be authorised by a Directorate Support Manager or third tier officer while a new approver must be authorised by a third tier officer. It is important that authorised users are granted appropriate access levels commensurate with their role, whilst simultaneously giving due consideration to segregation of duties. A unique user ID and a temporary password, which must be changed when the user first logs in, are provided by the FST. Changes to requisitioner or approval details require to be notified and authorised in the same way as new users.

2.3.2 As at 17 January 2018, there were 1,361 active users, each with a unique user ID. 24 users had administrator rights, however, these have variable permissions dependent on the user's role: for example, some Finance staff can only reset passwords. Only the FST have full administrator rights to allow them to manage the system. A review of the administrator rights granted showed them to be appropriate with the staff role. A review of orders raised between 1 April and 31 December 2017 identified that that only three orders had been raised by system administrators and these were for Services related to the PECOS or eFinancials systems, which related specifically to the member of staff's role within the FST. No orders were approved by an administrator.

2.3.3 The system maintains an automatic audit trail of user activity which the user cannot amend or delete, however these are not capable of being reported locally. Each order has an online audit trail recorded and is visible on-screen for enquiry purposes. It details the progress of the procurement journey, with the date, user and action undertaken. A separate audit log is reportable for any tasks undertaken by system administrators, when setting up new users, suppliers or other system management tasks. The log is not reviewed, and the FST was unaware of its existence until the audit was undertaken. The absence of review of system administrator activity increases the risk of error and fraud.

Recommendation
System administrator activity should be regularly reviewed by a Finance officer out with the Finance Systems team.
Service Response / Action
Agreed. In order to view the log in the system, system administrator access is required however a report will be extracted on a monthly basis and forwarded to a Finance Officer who is not an administrator.

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

2.3.4 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 system has a default 6 character password although this can be increased by system administrators. It does not force special characters but can enforce alpha/numeric requirements. The Corporate Information Management procedure requires passwords to be at least 8 characters long and contain a mixture of numbers, letters and special characters. Ensuring longer, complex passwords enhances the security over system access.

> **Recommendation**
> The system password requirements should comply with the Council's Corporate Information Management procedure.
>
> **Service Response / Action**
> Agreed. The system will be updated to require an 8 character alpha / numeric password.
>
> | **Implementation Date** | **Responsible Officer** | **Grading** |
> |---|---|---|
> | May 2018 | Finance Manager (Systems) | Important within audited area |

2.3.5   The system allows a user three attempts to log on before the account is locked, requiring a system administrator to unlock it. There is no written request required, and administrators will carry out the task based on a phone call or email from the user. The system then generates a random password and emails it direct to the email address held against that user. There are no records kept of password resets carried out and no review is undertaken to identify any patterns.

2.4   User Testing

2.4.1   As at 17 January 2018 there were 2,871 user records on PECOS: 1,361 active and 1,510 inactive. Roles include requisitioner, receiver, approver, administrator and enquiry only.

2.4.2   A sample of 5 PECOS users set up in the current financial year was selected and each was supported by a fully completed and authorised New User Form and approval limits were considered appropriate.

2.4.3   It is the employing Service's responsibility to notify the FST when a member of staff with PECOS access leaves. Details of leavers recorded in the payroll systems for the current financial year was extracted and compared by name to the active PECOS users. 43 active users on PECOS appeared to have left the Council. While it is incumbent on Services to notify the FST of leavers, as there is no common identifier between payroll and PECOS (e.g. employee payroll number) it is not possible to run an automated check. The Service has advised that there is no available field in PECOS for this purpose.

> **Recommendation**
> The FST should consider carrying out regular user audits.
>
> **Service Response / Action**
> Agreed. An initial review of users for the purpose of removing leavers will be carried out once the Target Operating Model has been implemented. An annual user audit will be carried out subsequent to the initial review.
>
> | **Implementation Date** | **Responsible Officer** | **Grading** |
> |---|---|---|
> | June 2018 | Finance Manager (Systems) | Significant within audited area |

2.4.4   PECOS has a test / training version which is also hosted. The system supplier will upload any patches or improvements onto the test system and allow the FST to check that they work correctly using archived live data. Provided there are no issues then the FST will notify the supplier and the changes will be applied to the live system. It can also be used by users for training purposes as the access rights mirror the live system as does the user name and password.

2.4.5   The Finance Manager confirmed that results of testing are not fully documented prior to implementing system updates and upgrades. This increases the risk that system changes will not have been adequately tested resulting in unintended disruption to service users.

Recommendation
The Service should consider introducing a testing checklist for completion and approval prior to system changes being implemented.

Service Response / Action
The Service does not have the resources available to test all PECOS updates particularly with the very tight deadline given by the Scottish Government for applying these. Prior to general release for testing, specific local authority users have already tested updates and we tend to rely on that testing. The Service makes sure basic functions work prior to applying updates and upgrades and this will be documented.

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

2.5   Data Protection

2.5.1   The Council's Data Protection Policy requires that all staff who process personal information undertake specified Data Protection Training at the commencement of their employment and to complete regular refresher training thereafter.

2.5.2   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.

2.5.3   The FST has stated that it is not a requirement for new users accessing PECOS to have undertaken data protection training. However, Legal and Governance has confirmed that some data contained in the system would constitute personal data as defined by the Data Protection Act 1998. A sample of 25 employees who have access to PECOS were checked to ensure / ascertain if they had all completed Data Protection Training. Six had undertaken training although each worked in a Service where they would have access to other sensitive personnel information.

Recommendation
All employees accessing PECOS should complete Data Protection training.

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

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

2.5.4   Schedule 1 of the Data Protection Act 1998, principal 5, states "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes." The data held on PECOS has never been purged, therefore it holds data relating back to when the system was first used. Current requirements from HMRC are for purchase orders to be retained for six years to comply with VAT regulations. Therefore if personal data is being held beyond this, the Council is at risk of breaching principle 5 of the DPA.

2.6 Interfaces

2.6.1 The purpose of system interfaces are to update PECOS with new / amended catalogues and the eFinancials system with details of purchase orders raised and goods / services received.

2.6.2 Scotland Excel produces catalogues for suppliers who are part of Framework Agreements and is responsible for ensuring that the pricing and items contained within the catalogues are correct. CPS relies upon Scotland Excel's measures and does not undertake checks on the catalogues, which are copied into the correct format for PECOS by CPS staff and forwarded to the FST to be uploaded into the system. Catalogues for specialist goods are prepared by CPS Procurement Specialists in conjunction with appropriate Service Managers and are then forwarded for uploading in the same way.

2.6.3 Bulk uploads of orders placed on PECOS are done overnight, while ongoing variations or goods receipts are interfaced every 30 minutes. System e-mails are sent to an FST email address notifying them of a successful upload, or reporting and detailing any failures. The FST review the failure reports to ascertain the reason, and either notify the requisitioning Service to make a correction (e.g. incorrect financial code to be corrected), or where administrative action is required, make amendments to PECOS or eFinancials (e.g supplier closed in eFinancials but open in PECOS allowing order). The interface will not accept any non-active financial ledger codes, which will be reported as failures, and therefore no suspense entries will be generated.

2.6.4 A review of the successful and rejected interface reports for the beginning of January 2018 showed no rejections relating to the previous months. A sample of three weeks within January found that the same rejections were not remaining outstanding between weeks.

2.6.5 Orders and receipts interfaced from PECOS to eFinancials are placed in a holding area each day until 3.30 pm, when a "matching" job is processed. For an invoice to be processed successfully, the system will look for a three way match between the purchase order, goods received and invoice. If invoices relating to purchase orders placed through PECOS are matched, they will be accepted automatically for payment in eFinancials, once the invoice information is entered to the system.

2.6.6 The current error tolerance limit is £2 for all suppliers except a catering supplier, for which the tolerance level is £50. The tolerance limit has been set at this level following discussions with Services, who accept that there may be variances in the types of foodstuffs and quantities delivered from that ordered, and are satisfied with the tolerance level.

2.6.7 A reconciliation between PECOS and eFinancials is not carried out on a regular basis. Reliance is placed on the interface reporting being accurate. If at any point an invoice is

received and the matching process within eFinancials fails due to inconsistencies with the order within eFinancials then the FST will carry out a reconciliation check to ascertain the reason for the order not being rejected during the upload.

2.6.8　A sample of 45 orders (5 per month April to December 2017) was tested and it was confirmed that all details had been accurately transferred to the financial ledger, including the financial ledger code, supplier, goods / service description, and amount.

2.6.9　Reports of orders raised in November 2017 showed that 5,907 were raised on PECOS and 5,818 matched the e-financials data. The difference of 89 related to cancelled orders or orders which had not yet been approved.

2.7　Manual Data Input

2.7.1　Orders are all raised manually within PECOS which has mandatory fields along with drop down menus to facilitate data input.

2.7.2　In November 2017, the Council raised 5,907 orders to the value of £5,360.086 through the system. The system automatically allocates a purchase order number when the order is created, and orders cannot be deleted. Orders can either be approved and issued, cancelled, or remain incomplete. A review of the order number sequence found there were no gaps.

2.7.3　The PECOS system allows larger quantities to be receipted than had been ordered. These "extras" are not subject to the same approval process as the original order. However, payment for additional goods received will be limited to the payment tolerances described in paragraph 2.6.5, above.

2.7.4　Where an order is incomplete it will be highlighted in the requisitioner's PECOS workflow, making the user aware that work still has to be completed prior to it being issued. There is no overview by FST or Commercial and Procurement Services (C&PS) of orders that have not been fully completed. A report extracted from the system by Internal Audit indicated that some incomplete orders dated back years.

2.7.5　The Council has a combined PECOS / creditors new / amended supplier form (FST99A). The form is used to collect supplier details along with bank details, although this is only recorded in e-financials and not PECOS. It is also used by C&PS for establishing whether a supplier should be set up on the system for use, depending on whether Procurement Regulations have been complied with. The form is completed in part by the requisitioner and part by the supplier before being approved and passed to C&PS. If C&PS are satisfied that the goods / services are not already covered by an existing contract / framework and the justification is adequate, they will forward on through workflow to the payments section and FST, to set up the supplier in eFinancials and PECOS.

2.7.6　As at 23 January 2018, PECOS held 7,077 suppliers, of which 6,858 were active. In the current financial year (April to January) 326 new suppliers were set up in PECOS. A sample of 25 was tested and it was confirmed that the required information had been fully completed on the form, and the supplier details were correctly input to PECOS.

2.8　Performance Monitoring

2.8.1　The Scottish Government does not require performance information from the Council. The FST has stated the system has had no issues or extended downtime, and the main concern from users has tended to be in relation to internet performance as the system is hosted and accessed online.

2.9   Suspense

2.9.1   PECOS does not require correct financial ledger codes to be entered when an order is raised however the interface to eFinancials will only accept a valid ledger code. Therefore, no transactions which are accepted into eFinancials will have an invalid ledger code and no transactions will be posted to a suspense account as a result.

2.10   Business Continuity Planning / Confidentiality

2.10.1   PECOS is hosted by the developer on behalf of the Scottish Government. The Scottish Government website states that the system is backed up to a disaster recovery data centre in a separate location.

2.10.2   The Council's IT Operations Management Standard requires that where a 3rd party network provider supplies services it must be established at the outset that confidentiality, integrity and availability requirements can be met, and SLA and contracts are well defined. The Finance Service business continuity plan (BCP) identifies the PECOS supplier as a key supplier and therefore confirmation should be available that it has adequate business continuity arrangements in place of its own. This should be included within the service contract or a Key Supplier Business Continuity Planning Assessment Questionnaire should be completed by the supplier.

2.10.3   Finance had assumed the software license agreement covered both of the above requirements. However as a copy of the agreement is not held by the Council, this cannot be confirmed. Should the two requirements not be included then separate agreements will have to be entered into with the PECOS software provider.

2.10.4   The Scottish Government P2P Service Integration Support and Maintenance Agreement with the interface data centre supplier, responsible for converting PECOS files to a format ready for eFinancials, states that the terms and conditions applicable to the support agreement are as per the Scottish Government's P2P Service Management contract. Confidentiality and business continuity terms and conditions are not included separately within the signed contract with this supplier.

Recommendation

If required, a 3rd party confidentiality agreement and key supplier business continuity assessment questionnaire should be completed by the PECOS and interface software providers.

Service Response / Action

Agreed. This can be requested from the interface software provider / Scottish Government but implementation is dependent on their response.

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

---

AUDITORS: D Hughes
             A Johnston
             G Flood

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.