ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	22 February 2018
REPORT TITLE	Internal Audit Report AC1822 – YourHR
REPORT NUMBER	IA/AC1822
LEAD OFFICER	David Hughes
AUTHOR	David Hughes

1. PURPOSE OF REPORT

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

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 YourHR.

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. IMPACT SECTION

7.1 **Economy** – The proposals in this report have no direct impact on the local economy.

7.2 **People** – There will be no differential impact, as a result of the proposals in this report, on people with protected characteristics. An equality impact 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. The proposals in this report will have no impact on improving the staff experience.

7.3 **Place** – The proposals in this report have no direct impact on the environment or how people friendly the place is.

7.4 **Technology** – The proposals in this report do not further advance technology for the improvement of public services and / or the City as a whole.

8. APPENDICES

8.1 Internal Audit report AC1822 – YourHR.

9. REPORT AUTHOR DETAILS

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

ABERDEEN
CITY COUNCIL

Internal Audit Report

Corporate Governance

YourHR

Issued to:

Morven Spalding, Interim Head of HR
Simon Haston, Head of IT
Fraser Bell, Head of Legal and Democratic Services
Steven Whyte, Director of Resources
External Audit

Date of Issue: February 2018 **Report No. AC1822**

EXECUTIVE SUMMARY

YourHR is an employee self-service and electronic workflow system used by approximately 5,000 employees and Councillors to view recent payslips; view and update personal information; report health and safety incidents; claim and approve annual and special leave; claim and approve overtime; carry out performance reviews; and report on sickness absences.

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

The results of testing were generally satisfactory. Whilst recognising that the system is scheduled to be replaced by a new Human Capital Management system, recommendations have been made in relation to system audit trail reviews, data protection training, written procedures, records of system failures and faults, system access, reporting of health and safety incidents and accidents, reconciliations and data security. These have been agreed either for implementation within the current or future system.

1. INTRODUCTION

1.1 Effective and efficient Human Resource management and facilities can yield significant benefits across organisations.

1.2 YourHR is an employee self-service and electronic workflow system aiming to provide an array of financial and non-financial benefits:

- Cost savings through reduced administration of paper-based forms;
- Reduction in calculation errors and the misplacement of employee request forms;
- Automation of the workflow;
- Improved data accuracy; and
- Improved data protection.

1.3 The Council has in excess of 9,000 employees and produces more than 250,000 payroll and HR related transactions annually, including but not limited to:

- Annual/Flexi Leave;
- Expenses Claims;
- Sickness Absences; and
- Overtime Claims.

Prior to the launch of YourHR, the majority of these transactions were paper based, leading to a variety of processes throughout the Council and increased risk of error. YourHR aimed to standardise processes and reduce the administrative workload relating to payroll transactions this for the majority of staff.

1.4 YourHR was developed in-house by a project team using off-the-shelf development tools. YourHR currently has 4,997 active users who can perform tasks including: viewing their 12 most recent payslips directly; claiming, reviewing and approving overtime; viewing and updating personal information; reporting of health and safety incidents; claiming and approval of annual and special leave; performance reviews and development; and the reporting of sickness absences. The system was rolled out in four phases to employees who have a Council workplace email. For those ineligible for enrolment onto YourHR, the manual processes automated by YourHR remain in place.

1.5 The YourHR system can be accessed by any individual who is enrolled when either connected to the internal network through the Zone or through the employee's internet browser on personal devices. Usernames and passwords are required to be input for any access.

1.6 It is the current intent and plan for HR to replace the YourHR system with a new Human Capital Management (HCM) system which will be part of the new integrated payroll and HR system within the next 18 months.

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

1.8 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Morven Spalding, Interim Head of HR, Andrea Garden (Team Leader), and Lynn Ritchie (Information Systems Architect).

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Procedures

2.1.1 Comprehensive written policies and 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.

2.1.2 Process maps are available on the Zone for certain YourHR functions thought to be more complicated, such as reporting absences, however written procedures describing how to carry out standard functions within YourHR are not in place. With the system being replaced within the next 18 months, developing extensive written procedures for the system at this stage may not be an effective or efficient use of resources. Therefore, the recommendation below is made with reference to the new HCM system.

Recommendation
The Service should develop and approve readily available, comprehensive written procedures for the HCM system.

Service Response / Action
Agreed. Where there is a requirement for a procedure to be created the relevant function will arrange for this to be produced and made readily available.

Implementation Date	Responsible Officer	Grading
April 2019 but dependant on implementation of the new HCM System	Project Lead (HCM)	Important within audited area

2.2 System Supply, Development and Maintenance

2.2.1 YourHR was developed by an in-house team using software and hardware already owned by the Council. The system has been updated on an ongoing basis with new modules developed and implemented over the life of the system. A log is kept showing the outstanding, in progress and completed system development projects. All new features and alterations to the system are tested prior to live implementation within the YourHR test system, before being tested by a manager of an applicable service. The new module / update can then be rolled out to all YourHR users. This testing platform aims to ensure that the system is fully functional prior to going live.

2.2.2 Two Business Analysts within the Council have administrative status with regard to YourHR and are responsible for the corrective measures required when any issues occur. System failures or issues are logged with ICT and steps are taken by Business Analysts to correct the issues.

2.2.3 Best practice is to record any system issues in a failure and / or fault log. This log allows for the tracking of issues and can enable easy identification of fault or issue trends. A log should contain information regarding the nature and extent of the issue, the date and time the issue occurred and was logged, the resolution and the date and time the issue was resolved. Failing to keep such a log risks issues not being resolved in a timely manner. The previous Project Lead, based in HR, maintained an up-to-date log, however, since responsibility for the system transferred to IT, no records now exist or are being maintained.

Recommendation
The Service should keep a record of all system failures and faults.

Service Response / Action
Agreed. System failures and faults will be recorded on service now.

Implementation Date	Responsible Officer	Grading
January 2018	Information Systems Architect	Important within audited area

2.3 System Access

2.3.1 YourHR provides a portal allowing employees to view and edit their personal information. Due to the personal nature of the information stored within the system it is imperative that adequate controls exist to prevent inappropriate access to the data.

2.3.2 Users can access the system either directly through the Zone or through the employee's internet browser on personal devices. The individual must then enter both their workplace email address or username and their personal password to complete the login. It is Council Information Security policy that passwords must contain at least 8 characters and contain at least one letter, number and special character. YourHR conforms to these requirements.

2.3.3 The system is also designed to block individuals from accessing the system following multiple incorrect password attempts. This is to prevent individuals from guessing passwords and gaining inappropriate access to the system and viewing the information of another individual. A call must then be logged to AskHR to unlock the account and an email containing a time-sensitive validation code is then sent to the individual's workplace email to reset the password. The password must then be reset by the individual within 20 minutes or the validation code will expire and another call must be logged. Internal Audit tested password security by using the test system and attempting to gain access using the incorrect password for the test user account. Following 4 failed attempts, the system locked out the user and even when the correct password was subsequently used, access was not gained.

2.3.4 All incorrect login attempts are recorded by the system allowing for the system administrator to perform audits of the login attempts. These are performed on an ad hoc basis by the Service. No reports of findings are produced from these.

Recommendation
Consideration should be given to the reporting requirements for and over the new HCM system.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
April 2019 but dependant on implementation of the new HCM System	Project Lead (HCM)	Important within audited area

2.3.5 A timing out control ensures that if a user is inactive for 20 minutes (45 minutes in the performance review and development section) they are automatically logged out. When making a timing out decision the system only considers a user accessing different screens as active, and not typing on a screen, allowing enough time for activities to be completed, whilst not being excessive and unnecessarily long. Internal Audit examined the timing out

features by leaving the test system logged in and inactive. The system timed out appropriately.

2.3.6 One of the key benefits of the YourHR system is the ability for individuals to update their personal information immediately. In order to ensure that changes are appropriate and made by the correct individual, an email is sent to the individual's workplace email as confirmation. In order to ensure that this control is robust, the system does not allow individuals to alter the email address within the system.

2.3.7 An additional safeguard is present where an individual wishes to change their bank details. The existing bank information is hidden from view and prior to making any change to bank details, the individual must first enter their current details. Failure to do this correctly will not allow the employee to enter the new details. As with all other changes to personal information, an email confirmation of the changes is then sent to the employee, however this does not include the bank details for security reasons.

2.3.8 When an individual joins the Council, ICT will contact the HR Service Centre (HRSC) with the new employee's email address. This will then be input to the PS enterprise (PSe) HR system and an account can then either be created in YourHR by HRSC or the employee upon their employment commencing. Access rights are then assigned by HRSC that are appropriate according to their job title, whether they are considered a line manager or whether they are considered a budget holder. The roles which can be assigned are: Employee, Manager, HRSC, Payroll, Business Partner Team, Service Admin or System Admin. A sample of 5 new starts within the Council from April – November 2017 was tested and this confirmed that they were granted appropriate access rights and that this was done timeously.

2.3.9 Where an individual leaves the Council, their details are updated in PSe and an overnight data upload removes access from YourHR from the appropriate date. Internal Audit tested whether any access to the system has been gained by the individual following leaving the Council through inspection of the audit trail and whether the user was still listed as active on the active user register. A sample of 5 leavers from the Council during the period April 2017 to November 2017 was tested. None of these were included in the active user logs, and according to the audit trail none had gained access to the system after they left the Council. No exceptions were therefore noted.

2.3.10 One third party external organisation to the Council has use of YourHR – Bon Accord Care. Bon Accord Care has full functionality within the YourHR system with the only difference being how admin and line manager access levels are assigned due to the differences in organisational structure from the Council. No explicit review is made by the Council over the information being processed on YourHR by Bon Accord Care as this is an Arm's Length External Organisation (ALEO). Bon Accord Care has no access to the Council employees and the two are kept distinctly separate through the user access rights.

2.4 Data Input and Processing

2.4.1 Data is transmitted from PSe to YourHR overnight, meaning that when an individual logs on to YourHR the next day, they see a snapshot of their information as it was overnight. When an employee updates any information in YourHR or claims overtime or special leave, then the information is transferred to PSe instantaneously. This then provides HR and payroll with up to date information on each individual.

2.4.2 Where an employee wishes to raise an overtime, unpaid or annual leave claim, make a change to their personal details, and where a health and safety incident report is being made then an electronic form (eForm) must be completed. A sample of 8 of each of these changes was tested and confirmed that the forms were effecting the required change or

reports within the appropriate corresponding system. In total a sample of 40 eForms were tested across an 8 month period (April – November 2017).

2.4.3 Health and Safety incidents and injuries are reported through YourHR by an individual's operational line manager or by a nominated employee within the injured party's Service. No issues were noted in the health and safety reporting through YourHR; all reports are investigated by the individual who raises the report and these are reviewed by HSW and reported as appropriate through RIDDOR or to HSE. The system features functionality for each Service to download all of the reports for their Service. This should then be cascaded down to managers to ensure awareness of health and safety issues and that any corrective measures can be taken in the workplace. However, whilst Services are running these reports, managers are not being made aware of outstanding incidents and these are not being fully investigated or completed correctly. This can result in matters not being closed in a timely manner by management.

Recommendation
Services should be reminded of their responsibility to cascade information regarding YourHR reported health and safety incidents throughout their Service.

Service Response / Action
Agreed. An e-mail will be sent out to Business Support managers/teams to remind them of their responsibility regarding YourHR reported health and safety incidents throughout the Service.

Implementation Date	Responsible Officer	Grading
January 2018	Team Leader (H&S)	Important within audited area

2.5 Audit Trail Functionality

2.5.1 Audit trail functionality exists within the system to allow the tracking of all logins and changes made and audit logs are reviewed by system administrators. However, system administrator activity is not reviewed as audit logs do not record changes made by system administrators.

2.5.2 Procedures require that if a system administrator wished to disable the audit trail functionality they must first receive approval from the Payroll Team Leader and / or the Information Systems Architect by way of an email request. However, it is possible to disable the audit trail without the knowledge of these individuals. In view of the system being replaced in the near future, no preventative control is recommended, however, an independent review of audit logs should be completed.

Recommendation
The Service should introduce an independent review over the changes made by system administrators. This individual should have no or limited access to the system and should be adequately knowledgeable to detect and highlight inappropriate actions within the system.

Service Response / Action
Due to the set-up of the system this may be difficult to achieve, but the Service will investigate whether this is possible.

Implementation Date	Responsible Officer	Grading
March 2018	Information Systems Architect / Team Leader (Payroll)	Significant within audited area

2.6 Data Protection

2.6.1 The Data Protection Act 1998 must be adhered to by the Council (Data Controller). The Data Controller has responsibilities under the legislation to protect personal and sensitive personal data of its employees and to ensure that such data is processed for its intended use only.

2.6.2 The Council provides three different courses that are relevant to the Data Protection Act 1998: 'Data Protection Essentials' focused on data protection, 'Employee Induction' which introduces the core Council policies including data protection, and 'For Your Eyes Only' which is an information security module.

2.6.3 The Council's Data Protection Policy (as approved by the Finance, Policy and Resources Committee on 15 September 2015) states that all employees who, as part of their role, are required to process personal information must undertake specific data protection training on commencement of their employment and undertake refresher training at appropriate intervals thereafter.

2.6.4 A sample of 10 employees was selected for testing to ensure this training was completed through an inspection of individual's training records. The following was noted in the testing:

- 8 of the sampled individuals have completed the 'Data Protection Essentials' module on OIL, 4 of which have completed this within the last three years;
- 1 employee joined the Council within the last year and completed training on Data Protection basics during the mandatory 'Employee Induction'; and
- 1 employee completed the 'For Your Eyes Only' training module in 2008 and has since received no further training.

2.6.5 All staff members in HR and payroll, and system administrators, have access to personal information. Therefore, appropriate training must be completed to comply with Council policy. Regular refresher training should also be being provided to ensure compliance is maintained.

2.6.6 Were a member of staff to act in breach of the Data Protection Act 1998 when performing their duties in processing information on behalf of the Council, the Council will be liable for any fines. With General Data Protection Regulation coming into force in May 2018, the maximum fine for the Council for a breach of data protection regulations will rise from £500,000 to €20,000,000.

Recommendation
The Service should consider whether refresher training on the 'Data Protection Essentials' module should be provided more regularly.

Service Response / Action
The Data Protection course is currently being rewritten in light of the changes resulting from the new General Data Protection Regulation (GDPR) obligations, which come into effect on the 25 May 2018. All employees will be required to complete the new course and clear instructions will be given as to the frequency employees will be required to refresh their knowledge and understanding.

Implementation Date	Responsible Officer	Grading
December 2018	Team Leader (OD) / information Manager	Significant within audited area

2.6.7 A detailed data protection review was undertaken across the Council as part of the Data Protection Audit (report AC1707).

2.7 Reconciliations

2.7.1 Reconciliations are a pivotal control in ensuring accuracy and completeness of information. However, the YourHR system provides no reconciliation functionality and no manual reconciliations are performed. System functionality should allow for data line items to be reconciled from the system to the source and vice versa. This can be achieved by either automated reconciliations initiated by the system, the use of bespoke middleware software or the ability to generate system reports which can then be reconciled back to the system manually. Any reconciling differences should then be investigated and corrected timeously.

2.7.2 The Service does perform a check over the data transfer to ensure that the file size being received by one system is the same size as the file being sent by the other. This is a high level review and provides no comfort that the detail contained within the files agree.

Recommendation
The Service should perform reconciliations over system data and should investigate and correct any reconciling differences.

Service Response / Action
The Service will investigate how to better the process and determine what further checks are required to be put in place to ensure data consistency and completeness between the two systems.

Implementation Date	Responsible Officer	Grading
May 2018	Information Systems Architect	Important within audited area

2.8 Performance Monitoring

2.8.1 Stability of an IT system ensures that the service provided by the system is regularly available and suffers few performance issues. A key method in achieving stability is to ensure that performance of each IT system is consistently monitored. With regard to YourHR there are two facets which are monitored for stability and performance.

2.8.2 The first of these is the overall server stability and performance which is managed for all Council servers by the external data centre provider. The second is the database and interface performance. This is monitored in-house by IT who can make ad-hoc adjustments to the system. As a means to introduce these changes and to monitor the system, YourHR is unavailable for access from 12-12.30pm and 5-5.30pm every day.

2.9 Security

2.9.1 When two systems interact as a means to transfer information, it is essential that the transfer is completed within IT security requirements. Both PSe and YourHR are internal systems protected by the overall IT firewall and no data is transferred out with this. Therefore for somebody to be able to intercept this data they would first be required to breach the firewall protecting all Council systems.

2.9.2 Data transferred between the systems is not encrypted and therefore were access gained through the firewall, the data transfer could potentially be intercepted. These data transfers can include certain sensitive personal information and therefore were a breach to occur there is no additional safeguards protecting the data being transferred.

2.9.3 The HCM system will combine both the payroll/HR aspects with the employee self service capabilities currently provided by YourHR in a fully integrated system. Therefore there

will be no data transfers between systems, however the Council should ensure that the information being held by the system and/or being transmitted to other systems is protected from interception.

Recommendation
The Service should consider encrypting the data being transferred between the systems as a safeguard to prevent any data transfer interception.

Service Response / Action
The use of SFTP (Secure File Transfer Protocol) instead of (File Transfer Protocol) FTP will be considered. SFTP encrypts data which is being transferred over a network, improving security when compared with FTP.

Implementation Date	Responsible Officer	Grading
March 2018	Information Systems Architect	Important within audited area

2.10 Business Continuity and Disaster Recovery

2.10.1 Disaster recovery and business continuity planning are integral parts of the overall risk management for an organisation. This aspect of risk management within the Council has been examined in more depth as part of the Major IT Business Systems Audit and Business Continuity Plans were audited in report AC1804. YourHR is considered one of the Council's top 20 most important systems and therefore is part of the first line of systems to be restored following any outage. Although not explicitly mentioned within the business continuity plan, YourHR is considered a part of the PSe system by the Council and is included in the disaster recovery for this.

2.10.2 System backups are performed by the Council's data centre provider with backups being held at an external location. This ensures that were an incident to occur impacting the data held onsite by the Council, then data would not be lost and could be recovered from this external source, reducing downtime.

2.10.3 In a previous audit of the YourHR system in 2013 it was identified that all development software was stored on two PCs held in Marischal College with no external backup. The Service has confirmed that this is now backed up into the test system, which is then included as part of the backups highlighted above.

AUDITORS: D Hughes
A Johnston
J Grigor

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.