Aberdeen City Council

Your HR System – Key IT and Access Controls

Internal Audit Report
2012/2013 for Aberdeen
City Council

April 2013

Contents

1. Executive Summary

Report classification	**Total number of findings** ← Section 3 →				
	Critical	**High**	**Medium**	**Low**	**Advisory**
Medium risk					
Control design	-	-	1	2	-
Operating effectiveness	-	-	1	-	-
Total	-	-	**2**	**2**	-

Summary of findings

1.01 Aberdeen City Council (ACC) processes approximately 250,000 transactions per annum in respect of staff annual leave, sickness absence, overtime and mileage claims. The processes are paper based relying on manual authorisation and submission of documents among various teams in the Council.

1.02 The Council is currently developing a self service portal interface, titled 'Your HR' that will provide employees with pay details online, replacing the paper forms and processes with electronic forms and agreed workflow to achieve improvements from an efficiency and effectiveness perspective. The system has been developed by an in-house project team using standard web browser tools.

1.03 The overall purpose of this internal audit review was to assess the design and operating effectiveness of the key controls in place over Your HR system in relation to system development and system access. Certain areas of good practice were identified such as:

- A system development process has been documented for Your HR
- The password requirements for accessing Your HR are in line with the Council's ICT Good Practice Guidelines and employees must first be logged in to their Novell profile.
- System development access is restricted to two individuals. The database is password protected and is changed every three months in accordance with the Council's ICT Good Practice Guidelines and when a staff member who has access to the system leaves the organisation.

1.04 We did not identify any critical or high risk findings during the course of our review. However we have made two medium risk recommendations and two low risk recommendation, with the intention of improving the general governance and procedures in place surrounding Your HR:

- The IT Project Team Leader maintains an issue log in which concerns, change requests, information and queries are documented. The issue log was kept up to date until the end of December 2012; however since this period, due to other commitments and staffing issues, the log has not been kept up to date (medium risk).
- The communication protocol for Your HR is planned to change from 'http' to 'https'. This would mean that an employee would be able to access their Your HR profile from a different computer to their own. Essentially this means that there would be one less control in place regarding access to the system as there would be no requirement to be logged in through the individual's Novell log in before accessing Your HR (medium risk)
- The Your HR database is only backed up with ATOS, an external server provider, on a weekly basis (every Friday). The system development work is stored on two PCs which are located in Marischal College and this information is not backed up. If the computers were to be damaged or destroyed there is a risk that all the system development work would be lost (low risk);
- There is a Project Board in place however there are no formal terms of reference for this Board that outline its role and remit and consequently there is no formal process which details how system development should be approved. Recent Project Board minutes from December 2012 identified this weakness and the Board is seeking to make improvements (low risk);

Management comments

1.05 (Recommendation 3.01) The Project Leader uses the Issue Log as a daily log. All major issues and change requests especially where impacting on time, quality, cost or the PSE payroll system will be recorded. In future the Project Leader's daily log will be recorded as the Issue Log as and when appropriate.

(Recommendation 3.02) This matter will be discussed and risk assessed with the ICT Service. No such event has taken place to date and there have been ICT failures over the past 12 months which has not affected the integrity of any data held on the PC's in question. It is suggested that albeit foreseeable this risk is minor as a maximum one week's development work would be lost if PC's were damaged or the Database corrupted and such a likelihood is also low.

(Recommendation 3.03) It is believed the recommendation of having two levels of password or PIN security must be balanced against potential dissatisfaction with users perceptions of 'yet another password' which will have negative effect on buy-in and ease of use of YourHR. Staff will be encouraged to keep passwords confidential and to regularly change them.

(Recommendation 3.04) This recommendation is accepted but it should be noted decisions are made following presentations to CMT out with the Project Board that effect the content and sequencing of the project. Work is underway to increase the representation on the Project Board by Senior Management and for the formal proposal of changes to the project be discussed and approved at the project board.

2. Background and scope

Background

2.01 Aberdeen City Council (ACC) processes approximately 250,000 transactions per annum in respect of staff annual leave, sickness absence, overtime and mileage claims. The processes are paper based relying on manual authorisation and submission of documents among various teams in the Council.

2.02 The Council is currently developing a self service portal interface, titled 'Your HR' that will provide employees with pay details online, replacing the paper forms and processes with electronic forms and agreed workflow to achieve improvements from an efficiency and effectiveness perspective. The system has been developed by an in-house project team using standard web browser tools.

2.03 Online access enabling staff to view their own employee data, amend their bank account details, and obtain payslip details electronically is currently available to all Corporate Governance Service staff and managers across all Council Services. There are further plans in place to roll out modules for travel and subsistence and absence recording in the future and to roll out the system to other staff within Aberdeen City Council, during 2013/14.

System development and governance

2.04 A system interface exists between Your HR and the PSE payroll system to ensure that any changes to standing data on Your HR will be reflected in PSE, and are therefore reflected in the pay run each month. The database which stores the data from Your HR is backed up on a weekly basis by the Council's third party server provider - ATOS. The database also includes data such as staff performance and evaluations which is not replicated on PSE.

2.05 Initial testing of Your HR was completed in a test environment within a small group that included the IT Project Team Leader and the system developers. During the initial stages of the system going live it was noted that one serious breach of data occurred since the introduction of the Your HR system, which involved an employee's personal details. Once identified, the breach was recorded and corrected immediately and a report was issued outlining the proposed measures to prevent a similar breach occurring in the future. One of the measures introduced was the development of a 'kill switch'. In any instance of a suspected data breach the kill switch can be initiated which will prevent employees from logging onto the system while the team work on solving the problem.

System Access Controls

2.06 Your HR identifies if an employee is accessing it for the first time and automates a passcode which is sent to the employee's email. The employee then enters this unique passcode and, when it has been accepted, is immediately prompted to create a new password in accordance with the Council's ICT Good Practice

Guidelines. An employee can only access their Your HR profile if they are logged into their own Novell system. There are no parameters set up to force a change in the Your HR password periodically, as the Novell password is set up to require a change every three months.

2.07 After logging into Your HR, there is a further control in place surrounding bank details. If an employee wants to change their bank details they must first enter their sort code and account number of the account that is currently registered within the system. Therefore, even if an individual had managed to get through to this point with the log in details for both the Novell system and Your HR, if they then wanted to change the bank details, they would also have to be in possession of the original sort code and account number of the relevant account. In addition to these controls, if an employee changes any of their personal details a confirmation email is sent to that employee confirming that this change has been made. Exception reports showing all changes made to employee details through Your HR are not produced, however, mitigating controls are in place which ensure that employees are able to trace any changes that have been made, i.e. through automatic emails and through a change log on the front page of Your HR once an employee has logged in.

2.08 As the system is still in its early stages there are no super-users for the system. There are two system developers who have access to the Your HR database. The database is password protected and is changed every three months in accordance with the Council's ICT Good Practice Guidelines and when a staff member who has access to the system leaves the organisation. The database is also only accessible from the two PCs in Marischal College which are assigned to the two developers.

Scope and limitations of scope

2.09 The detailed scope of this review is set out in Appendix 2. The review considered the design and operating effectiveness of the key controls in place over the operation of the Your HR system in relation to system development and system access. Due to Data Protection requirements it was not possible to gain access to the personal details of employees (such as bank details) in order to test the accuracy of the data that was transferring between Your HR and the PSE payroll system.

3. Detailed findings and recommendations

3.01 Formal Documentation of Changes – operating efficiency

Finding		
The IT Project Team Leader for Your HR maintains an issue log, documenting all issues, changes requests and queries. The log shows the issue when it is first raised and then documents its progress and final outcome. It was noted that this log has been kept up to date until the end of 2012. However, due to staffing and time constraints, not all issues have been documented in the issue log since January 2013.		
Risks		
It may not be possible to verify who approved changes to the system if they have not been logged. Serious issues may not be followed up if they are not formally documented.		
Action plan		
Finding rating	**Agreed action**	**Responsible person / title**
Risk rating: Medium	Officers will ensure that issues and changes relating to the system are documented per agreed procedures. The Project Team Leader has been assigned the administrative responsibility in relation to this and will update the log with any issues, change requests of queries on a regular basis.	IT Project Team Leader **Target date:** Immediate and ongoing

3.02 System Backup – control deficiency

Finding

The Your HR database is only backed up with ATOS, an external server provider, on a weekly basis (every Friday). This includes data such as staff performance and evaluations which is not replicated on PSE.

The system development work is stored on two PCs which are located in Marischal College and this information is not backed up. If the computers were to be damaged or destroyed there is a risk that a substantial proportion of system development work could be lost. In this event the system would continue to function in its current form. However in order for any further system development work to take place, the entire system would need to be rebuilt.

Risks

- There is a risk that if the Your HR database was damaged or corrupt up to a week's worth of data could be lost.
- If a situation arose where the two PCs in Marischal College were damaged or destroyed, the whole system development process would have to be rebuilt which would represent a loss of a considerable investment of time and money.

Action plan

Finding rating	Agreed action	Responsible person / title
Risk rating: Low	Management will consider whether to back up the database more frequently than once a week. This will include an analysis of costs compared with anticipated benefits to determine whether it would be appropriate to increase the frequency of back-ups. This will be discussed and risk assessed with the ICT service. It is noted that although it is the Council's policy to not further back up the system development which is stored on the two PCs in Marischal College, it would be advisable to make every effort possible to back-up the development tools in some way.	HR Manager & ICT Account Manager **Target date:** 30 September 2013

3.03 HTTPS Protocol – control deficiency

Finding		
It is anticipated that the Your HR system will use a 'https' protocol in the future, as opposed to the 'http' protocol which is currently used for the system. Whilst https is generally considered more secure than http, the change will have an impact on the controls currently in place surrounding access to the Your HR system. The current system ensures that an employee can only access their Your HR profile if they are firstly logged onto their Novell system. This mitigating control will be removed if and when the https protocol is introduced, meaning that an employee would be able to log in from another employees desktop. Additionally, users are not prompted to change their Your HR password periodically as they are already required to change their Novell log in.		
Risks		
Those with proxy access to others email accounts may be able to obtain access to their Your HR profile by requesting a password reminder to be sent to their email address.		
Action plan		
Finding rating	**Agreed action**	**Responsible person / title**
Risk rating: Medium	Employees will be encouraged to keep passwords confidential and to regularly change them. Management will consider putting an additional level of security in place in order to access the most personal data located in the Your HR system. For example another pin or password could be introduced within the system for accessing online payslips and other sensitive information. This will be balanced with the potential negative perception if too many passwords or pins are required.	IT Project Team Leader **Target date:** 30 September 2013

3.04 Project governance – control deficiency

Finding
There is a project board in place to oversee the development of your HR and the subsequent roll out across the Council. It was acknowledged in December 2012 that the project board needed a formal terms of reference, to clarify the boards role and remit including how systems developments would be approved. As a result an implementation plan was drafted and approved by the project board in March 2013. However, from review of the minutes of the project board and supporting papers it is noted that it would still be beneficial to further define the role and remit of the Board, and who should be involved in the development process and at what stage should clearly be recorded.
Risks
Without a formal process or chain of command in place there may be the possibility that a change to the system could be developed without formal approval which is later found to be an inefficient use of resource or that does not function properly.

Action plan

Finding rating	Agreed action	Responsible person / title
Risk rating: Low	Management should formally document the role of the Project Board in the development of the Your HR system and establish clear decision levels across the team. Whilst some development changes may not be significant, it would establish improved project governance if more substantial changes were formally proposed and approved at Project Board level.	Project Sponsor **Target Date:** 30 September 2013

Appendix 1 – Basis of our classifications

Individual finding ratings

Finding rating	Assessment rationale
Critical	A finding that could have a: • ***Critical*** impact on operational performance; or • ***Critical*** monetary or financial statement impact; or • ***Critical*** breach in laws and regulations that could result in material fines or consequences***;*** *or* • ***Critical*** impact on the reputation or brand of the organisation which could threaten its future viability.
High	A finding that could have a: • ***Significant*** impact on operational performance; or • ***Significant*** monetary or financial statement impact ; or • ***Significant*** breach in laws and regulations resulting in significant fines and consequences ***;*** *or* • ***Significant*** impact on the reputation or brand of the organisation.
Medium	A finding that could have a: • ***Moderate*** impact on operational performance; or • ***Moderate*** monetary or financial statement impact; or • ***Moderate*** breach in laws and regulations resulting in fines and consequences; or • ***Moderate*** impact on the reputation or brand of the organisation.
Low	A finding that could have a: • ***Minor*** impact on the organisation's operational performance; or • ***Minor*** monetary or financial statement impact; or • ***Minor*** breach in laws and regulations with limited consequences; or • ***Minor*** impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Report classifications

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification	Points
Low risk	6 points or less
Medium risk	7– 15 points
High risk	16– 39 points
Critical risk	40 points and over

Appendix 2 – Terms of reference

Background

Aberdeen City Council processes approximately 250,000 transactions per annum for annual leave, sickness absence, overtime and mileage claims. The processes are paper based relying on manual authorisation and transmission of documents among various teams in the Council.

The Council is currently developing a self service portal interface, titled Your HR System that will provide employees with pay details online, replacing the paper forms and processes with electronic forms and agreed workflow to achieve improvements. The system has been developed by an in-house project team using standard web browser tools.

On-line access enabling staff to view their own employee data, amend their bank account details, and obtain payslip details electronically is currently available to all staff of the Corporate Governance Service, and managers in the other Council Services. The current priority is to roll out the Personal Review and Development module to all Services by end of March 2013, and thereafter roll-out modules for travel and subsistence and absence recording.

Scope

We will review the design and operating effectiveness of the key controls in place over the operation of the Your HR system. The sub-processes included in this review are:

Sub-process	Control objectives
System Development	• Data migrated onto the Your HR system is complete and accurate
	• A system development process has been documented for the Your HR system
	• Only approved changes to the Your HR system are migrated into production
	• User acceptance of development is performed prior to go live

	• Procedural guidance and user training has been developed for Your HR and a procedure has been developed for dealing with queries
System Access Controls	• Appropriate user access is granted and employees are only able to view their own personal details
	• Those with super user access are not able to view or amend employee details
	• Any automated emails generate with employee passwords are secure
	• Compliance with ICT policy regarding use and change of passwords
	• Review of exception report covering amendments to personal details.

Limitations of scope

The scope of our review is outlined above. This review will not provide assurance on the adequacy of arrangements for rolling out the system. Testing will be undertaken on a sample basis. Due to Data Protection issues it was not possible to gain access to the personal details of employees in order to test the accuracy of the data that was transferring between Your HR and the PSE payroll system.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the systems access and development controls for the Your HR system through discussions with key personnel, review of systems documentation and walkthrough tests where appropriate.
- Identify the key risks in respect of Your HR system development and access.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the key controls on a sample basis.

Appendix 3 - Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken a review of Your HR system, subject to the limitations outlined below.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls relating to Your HR is as at March 2013. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.