ITEM No …6….

REPORT TO: **SCRUTINY COMMITTEE – 27 JUNE 2018**

REPORT ON: **INTERNAL AUDIT REPORTS**

REPORT BY: **SENIOR MANAGER – INTERNAL AUDIT**

REPORT NO: **205-2018**

1.0 PURPOSE OF REPORT

To submit to Members of the Scrutiny Committee a summary of the Internal Audit Reports finalised since the last Scrutiny Committee.

2.0 RECOMMENDATIONS

Members of the Committee are asked to note the information contained within this report.

3.0 FINANCIAL IMPLICATIONS

None

4.0 MAIN TEXT

4.1 The day-to-day activity of the Internal Audit Service is primarily driven by the reviews included within the Internal Audit Plan. Broadly, on the completion of a specific review, a report which details the audit findings and recommendations is prepared and issued to management for a formal response and submission of management's proposed action plan to take the recommendations forward. Any follow-up work subsequently undertaken will examine the implementation of the action plan submitted by management.

4.2 Executive Summaries for the reviews which have been finalised in terms of paragraph 4.1 above are provided at Appendix A. Within each Executive Summary the prime aim is to provide both Elected Members and management with key information which includes the reason for undertaking the review, a summary of financial data and statistics, the areas encompassed within the review and specific areas which were excluded, the principal audit objectives, an audit opinion on the adequacy of the systems and control framework of the area reviewed, the key conclusions based on the audit findings and recommendations and a summary of management's response to the audit report. The full reports are available to Elected Members on request.

5.0 POLICY IMPLICATIONS

This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti-Poverty, Equality Impact Assessment and Risk Management. There are no major issues.

6.0 CONSULTATIONS

The Chief Executive, Executive Director of Corporate Services, Head of Corporate Finance and Head of Democratic and Legal Services have been consulted on the content of this report.

7.0 BACKGROUND PAPERS

None

Pamela Redpath, Senior Manager – Internal Audit DATE: 6 June 2018

Appendix A

i) INTERNAL AUDIT REPORT 2016/30

Client	**City Development**
Subject	**Occupational Road Risk**

Introduction

A review of the arrangements in place within the Council to mitigate occupational road risk was part of the planned internal audit work.

The Scottish Government, together with its road safety partners, is committed to achieving safer road travel in Scotland and in 2009 published a Framework for improving road safety in Scotland to 2020, including casualty reduction targets for the period 2010 to 2020. A mid-term review in 2015 established that the Framework remained on target to achieve these reductions, however more recently statistics have reported an increase in road deaths. When the Framework was launched, one-third of all road crashes involved someone who was driving for work purposes and more employees were killed in 'at work road accidents' than in all other occupational accidents. It is not only commercial drivers who are at risk. People who are required to drive their own cars for work are also at risk.

Employers have a duty of care to employees driving for work under health and safety law. They also have duties under road traffic law. Both management and employees can be prosecuted for road traffic crashes involving work-related journeys, including employees driving their own vehicles. Under the Health and Safety at Work etc. Act 1974, there is a requirement for any organisation employing five or more people to have a written policy statement on health and safety, which should cover work-related road safety. In the case of work-related road incidents, organisations are required to provide evidence that they have taken reasonable steps to adequately discharge their duty of care.

Dundee City Council’s Occupational Road Risk policy and guidance were updated in August 2017. The guidance, developed to support those with responsibilities under the Council’s Occupational Road Risk Policy, covers all drivers on Council business driving either their own vehicle or a Council vehicle.

Following the fatal accident inquiry into the 2014 Glasgow bin lorry accident, the Sherriff made a number of recommendations to Glasgow City Council which were subsequently distributed to all Council Chief Executives. Following this, revised practices have been put in place within Dundee City Council for vehicle checks as well as medical requirements through the recruitment and selection arrangements.

Scope and Objectives

To review the Council's revised approach to mitigating occupational road risk and ensure that it is in line with recognised good practice in this area.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- Steps should be taken to complete the service roadshows promoting the revised Occupational Road Risk Policy and Guidance as soon as possible. Consideration should be given to issuing a supplementary “all staff” communication bringing the Policy and Guidance to the attention of employees who drive on Council business.
- The Fleet Manager should ensure that all managers within the Council are aware of the Council’s approach to the checking of driving licences for staff who drive on Council business. In addition, the Fleet Manager should ensure that there is clarity surrounding how the checking service should be used, including the frequency of checks carried out, how employees with penalty points and potential bans from driving will be regularly checked and how managers are notified of the results.

ii) INTERNAL AUDIT REPORT 2016/30 (Cont'd)

Conclusion (Cont'd)

- Managers with responsibility for fleet vehicles requiring a pre-start check should be reminded of their monitoring responsibilities, ensuring that these checks are being undertaken. For the central pool car vehicles, including the electric vehicles, the information in the Occupational Road Risk guidance and supplementary information on ONE Dundee for booking a pool car should be updated to ensure this is consistent and reflects current operational practice.
- The Fleet Manager should take steps to raise awareness of the procedures to be followed when drivers accrue 6 or more penalty points or have 3 or more "at fault" accidents within 2 years and put in place arrangements to periodically monitor compliance with those procedures.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Executive Director of City Development and the Executive Director of Corporate Services and appropriate action agreed to address the matters raised.

ii) INTERNAL AUDIT REPORT 2017/07

Client	**Corporate**
Subject	**Lone Working**

Introduction

A review of the lone working practices and procedures in place for Dundee City Council employees was part of the planned internal audit work.

Whilst there is no legal prohibition on working alone, the broad duties of the Health and Safety at Work etc. Act 1974 and the Management of Health and Safety at Work Regulations 1999 still apply. In particular, Section 2 of the 1974 Act sets out a duty of care on employers to ensure the health, safety and welfare of their employees whilst they are at work. Regulation 3 of the 1999 Regulations states that every employer shall make a suitable and sufficient assessment of the risks to the health and safety of its employees whilst they are at work and the risks to the health and safety of persons not in its employment but arising out of, or in connection with, service delivery.

In practice, lone workers are broadly defined as those who work alone without close or direct supervision. The requirements under the legislative framework in respect of lone working include identifying hazards, assessing the risks involved and putting measures in place to avoid or control the risks. Control measures may include instruction, training, supervision and protective equipment. In addition, organisations should take steps to check that the control measures are being followed and undertake a periodic review of lone working risk assessments to ensure that they remain appropriate.

In the context of the scope of this review, some employees are required to visit client's properties alone, such as Housing Officers and Social Workers. In addition, some employees are normally required to work on their own, such as Sheltered Housing Wardens, Home Care Workers and Construction Services tradesmen. It is, therefore, particularly important that appropriate arrangements are in place.

Scope and Objectives

Risk based assessment and review of the arrangements in place to deliver a safe working environment for employees who are required to work alone.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- The Council's corporate Guidance on Lone Working and Violence (Lone Working Guidance) should be reviewed and updated where applicable. Each strategic Council service should consider whether or not it is necessary to have its own service-specific guidance and, if so, document appropriate procedures in line with the Lone Working Guidance. For individual service areas / teams that have, to date, not developed operational lone working arrangements, these should be developed and documented as soon as possible in line with the recommended key controls detailed in the Council's Lone Working Guidance.
- Each service should identify and record all lone working posts / roles with a view to ensuring that appropriate lone working arrangements (risk assessments and operational guidance) are in place.
- A decision should be made regarding whether or not the alert systems maintained by individual services, in addition to the Council's Potentially Violent Persons Database (PVPD), are considered necessary. In addition, corporate guidance should be developed surrounding the length of time individuals should be recorded in the PVPD (and individual service systems as appropriate), review periods and when / how individuals should be informed that this is the case.

ii) INTERNAL AUDIT REPORT 2017/07 (Cont’d)

Client	**Corporate**
Subject	**Lone Working**

Management Response to the Audit Report
The audit findings and recommendations were formally reported to the Executive Director of Corporate Services and the Executive Director of Neighbourhood Services and appropriate action agreed to address the matters raised.

iii) INTERNAL AUDIT REPORT 2017/11

Client	**Corporate**
Subject	**User Access Levels**

Introduction

A review of the Council's policies, procedures and controls with regards to user account management to ensure that these are in line with recognised industry practice was part of the planned Internal Audit work.

User access controls are recognised as key information security controls for the Council in protecting the confidentiality, integrity and availability of information. User access levels are used to restrict access to, and the ability for individuals to read and or amend, information. It is important that user access is maintained in line with authorised business use and ensures appropriate segregation of duties between key activities (e.g. request and authorise a payment).

Consideration was given to the end to end user account lifecycle, considering the provisioning, maintenance and removal of access for both Council employees and third parties (e.g. system vendors and support). This audit focussed on the access to six Council's key systems, identified during the business continuity planning exercise.

Scope and Objectives

A high level review was performed of the appropriateness of user access levels and associated permissions for the following key Council IT systems as identified via the business continuity planning exercise:

- *CIVICA Financials (Debtors, Creditors and General Ledger), CIVICA Purchasing, Cash Receipting, NGA Northgate (Payroll)*, *Northgate Revenue + Benefits and CIVICA W2* (Electronic Document Management System for Revenues and Benefits)*.*

The objective was to verify that the access to these systems is controlled in line with internal policies and recognised good practice (e.g. ISO27001). The password controls in place for these systems have been assessed as part of a concurrent review on Data Security.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- *User Access Reviews* – To reduce the risk of unauthorised access via elevated privileges or dormant accounts, the Council could consider regular user access reviews for all systems in scope. This would enable system administrators, line managers and users to identify access permissions for active employees that are no longer needed, or for those accounts that are dormant / inactive. Priority should be given to the review of accounts with elevated permissions, e.g. privileged accounts. Frequency of review should relate to the risks associated with the use of the account or system. It is recommended that they occur on at least an annual basis.
- *Access Provisioning* – In order to reduce the risk of inappropriate approval levels being granted to employees during the account creation process, documentation should be created to detail the appropriate levels of approval needed to gain access to the systems. Segregation of duties should be documented within the procedures for granting users access to systems. This would help prevent any unwanted combinations of user account provisioning, whereby, the same system administrator is creating and setting access levels and authorisation limits for users. As a minimum, oversight from a system administrator should be performed to help identify and reduce any instances of elevated access to the system. In addition, user account provisioning could be established using blank user profiles or generic user profiles for their role or function. This would help reduce any elevated access that individual users may receive accidentally due to cloned accounts.

A number of good practice points were also highlighted, including that access to these systems requires a live Active Directory account, which if not used for more than 32 days is automatically disabled.

iii) INTERNAL AUDIT REPORT 2017/11 (Cont'd)

Client	**Corporate**
Subject	**User Access Levels**

Management Response to the Audit Report
The audit findings and recommendations were formally reported to the Executive Director of Corporate Services and appropriate action agreed to address the matters raised.

iv) INTERNAL AUDIT REPORT 2017/13

Client	**Neighbourhood Services and City Development**
Subject	**Festivals and Events**

Introduction

There are currently in the region of 1,700 events marketed on the Council's website, including a range of Council and third party organised activities.

The focus as a City for events and festivals are those events which:

- have economic benefits to the City by attracting visitors, increasing overnight stays or having employment benefits;
- promote and enhance Dundee's visibility and raise its profile as a vibrant, contemporary international City;
- are distinctive to Dundee by using the landscape, history, heritage or people of Dundee to make them unique; and
- are available to, and involve, members of the public in Dundee, or which inspire and involve local communities.

Within City Development, the Events Team works towards making Dundee a vibrant and exciting place to live, work and study by supporting a range of festivals and events across the City. The Team is responsible for delivering events such as the Easter fun day, fireworks displays and Christmas light nights. It also works closely with external event organisers to support and advise them on the delivery of other festivals and events such as Slessor Gardens concerts, Race for Life and community gala days. The scale of events ranges from multi-day events such as the Dundee Flower and Food Festival, to smaller community events such as the Broughty Ferry Gala Day.

Events take place at a number of outdoor locations and managed venues such as parks, City Square and Slessor Gardens. Third party organisations are required to complete an Event Application Form in advance of a proposed event which considers a number of factors including legal and licencing matters, health and safety and risk assessment. If approved, a Conditions of Use document is issued to event organisers.

Neighbourhood Services is also a key stakeholder for festivals and events from a community safety perspective and consequently should be involved from the outset providing specialist advice in respect of access to facilities, stages or other equipment as part of a festival or event.

Scope and Objectives

Review to assess the governance arrangements in place corporately to support festivals and events and ensure associated risks, including health and safety risks, are identified and mitigated.

Conclusion

The principal conclusion drawn from this review is that whilst there is basically a sound system of control there are some areas where it is viewed improvements can be made.

The main areas commented upon in the report are as follows:

- Although effective event management is in place, it is recommended that the end-to-end process is reviewed, with a view to defining and agreeing a new standardised procedure. Once agreed, the revised procedure should be communicated to key stakeholders.
- Senior Management within City Development and Neighbourhood Services should progress current efforts to define, agree and finalise roles and responsibilities. In addition, a Council-wide Events Team structure and associated partnership working arrangements should be established.

iv) INTERNAL AUDIT REPORT 2017/13 (Cont'd)

Client	**Neighbourhood Services and City Development**
Subject	**Festivals and Events**

Management Response to the Audit Report
The audit findings and recommendations were formally reported to the Executive Director of City Development and the Executive Director of Neighbourhood Services and appropriate action agreed to address the matters raised.

v) INTERNAL AUDIT REPORT 2017/20

Client	**Corporate**
Subject	**Data Security**

Introduction

A review of the Council's policies, operational procedures and system configurations in respect of the use of passwords to ensure that these are in line with recognised industry practice was part of the planned Internal Audit work.

Passwords are recognised as a key information security control for the Council in protecting the confidentiality of information. It is important for the Council to maintain a robust approach to passwords, considering both technical implementations and employee training and awareness.

This audit focussed on the security of six of the Council's key IT systems, identified during the business continuity planning exercise.

Scope and Objectives

Review of the internal controls in place to reduce the risk of unauthorised access of data through the use of passwords, including the resetting process. The following systems are considered in scope:

- *CIVICA Financials (Debtors, Creditors and General Ledger), CIVICA Purchasing, Cash Receipting, NGA Northgate (Payroll)*, *Northgate (Revenue and Benefits) and CIVICA W2* (Electronic Document Management System for Revenues and Benefits).

This review covered password policies, procedures, guidance and system configuration settings. The objective was to verify whether the password controls in place with regards to the in scope systems are adequate to prevent against unauthorised access. The appropriateness of user access levels and associated permissions for the same systems have been assessed as part of a concurrent review on User Access Levels.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- *Password Policy and Configuration Settings* – To reduce the risks associated with the use of weak passwords, the Council's Password Policy should be updated to reflect current industry guidance. In addition, to mitigate the risk of insecure password use, the deficiencies and gaps identified within Council system password configurations should be updated in line with the revised Password Policy.
- *Super User Accounts* – To reduce the risks associated with the sharing and uncontrolled use of super user accounts, additional controls should be enforced over the use of such accounts, including the use of unique accounts, disabling generic or shared accounts and regular password resets.
- *Password Reset and Transmission* – To reduce the risks associated with credentials being provided to unauthorised individuals, password reset and transmission procedures should be updated to validate the identity of the account holder and to avoid the use of generic temporary passwords.

Management Response to the Audit Report

The audit findings and recommendations were formally reported to the Executive Director of Corporate Services and appropriate action agreed to address the matters raised.

vi) INTERNAL AUDIT REPORT 2017/21

Client	**Corporate**
Subject	**Email Security**

Introduction

A review of the Council's arrangements and controls in place in respect of the secure transmission and receipt of email communications was part of the planned Internal Audit work.

Email communication presents a number of key information security threats to the Council. Phishing attacks and malware delivery typically occur via email, as a result it is critical to have an adequate level of technical control in place, such as anti-spam, anti-malware and anti-virus tooling to block or limit potentially malicious messages reaching Council employees.

Furthermore, often email may be used for the unauthorised sharing of information, either maliciously or due to employee error. It is important that technical controls, such as data loss prevention tooling, restrictions on online file sharing sites, or outbound email filtering and scanning are complemented by an adequate level of employee training and awareness to reduce the likelihood of such occurrences.

This audit considered the controls in place over both inbound (received) and outbound (sent) emails, accessed via Council computers or mobile devices.

Scope and Objectives

Review of the internal controls in place to reduce the risk of information, transmitted via e-mail, being accessed inappropriately. This included consideration of the internal controls in place to reduce the risk of email being used as a mechanism for the inappropriate access to and or sharing of data, or becoming a gateway to an attack on Council infrastructure and associated data. The following items were in scope:

- Security of information, transmitted via corporate email.
- Local, remote and mobile (mobile phone / smart phone / tablet, excludes laptops) access to email, including both corporate and personal devices.
- Policies, instruction, guidance, central and endpoint controls in relation to transfer of data via email, phishing emails and "click-bait" malware.

The objective of this review was to verify the level of protection offered to corporate email, and controls protecting employees and the Council from risks related to use of email.

Conclusion

The principal conclusion drawn from this review is that there are weaknesses in the system which should be addressed.

The main areas highlighted in the report are as follows:

- *Corporate email Data Loss Prevention (DLP*) - Ahead of the adoption of a new corporate email DLP solution, currently out for tender and due to be finalised by December 2018, measures should be considered to reduce the risk of data loss via email in the interim period. The Council should consider enabling email data loss detection and prevention functionality within the Council's existing WatchGuard filtering tool. Rules should be configured to detect data classification markings and other markers considered to be inappropriate for email transmission (e.g. bank details).
- *Personal email DLP* - To reduce the risk of potential data loss via personal email, or exposure to potentially malicious content, consider restricting access to, or enforcing additional control over, webmail e.g. outlook.com, gmail.com and other common online mail providers . Technical solutions exist that can allow access to personal email, whilst preventing the uploading or downloading of attachments, acting as both a DLP tool and providing an additional layer of anti-virus protection. It is understood that the Council's IT Service are currently trialling such

functionality internally on limited IT Service users. Once validated, this should be rolled out across all users.

vi) INTERNAL AUDIT REPORT 2017/21 (Cont'd)

Client	**Corporate**
Subject	**Email Security**

Management Response to the Audit Report
The audit findings and recommendations were formally reported to the Executive Director of Corporate Services and appropriate action agreed to address the matters raised.