Audit Committee
Tuesday 28 October 2014
Item No. 6

Midlothian Council

Review of Information Technology Control Environment

Gary Devlin
Engagement Lead
T: 0131 659 8554
E: gary.j.devlin@uk.gt.com

Raul Rodrgiuez
Technology Risk Services Manager
T: 0131 659 8526
E: raul.rodriguez@uk.gt.com

Contents

1 Executive Summary

1.1 Background

Each year, we ask our IT audit specialists to review the design and operating effectiveness of IT controls to assess whether there are any deficiencies which may have an impact on our financial statements audit.

As part of the Local Area Network's shared risk assessment process, we noted that the Council's "Big Move" project and rationalisation of city centre accommodation may have an impact on the way that council employees work. Revised workplace arrangements make greater use of home and mobile working, and cloud technology. We therefore asked our IT audit manager to review the Council's arrangements for data protection and information security arrangements.

1.2 Audit Approach

We performed a review of IT general controls. This included controls around logical access, change management and IT operations. We also assessed the operational effectiveness of security administration controls including users that have access to post invoices in the financial ledger.

1.3 Key findings

Section 2 of this report highlights the IT findings and recommendations emerging as a result of our review. We identified five weaknesses, all assessed as 'green', which means that they represent a control deficiency and have a risk of inconsequential financial misstatement.

1.4 Acknowledgement

Our audit involved discussions with a range of staff across the council. We would like to take this opportunity to thank those staff for their assistance and co-operation during the course of the audit.

2 Detailed findings

1	Deficiency	Posting of supplier invoices

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Supplier invoices are authorised through signature on the physical invoice. These invoices are sent to the Creditors team within the Finance department to be processed. Members of this team manually validate that invoices have been adequately authorised before releasing them for payment in the Integra system. We noted that one of the members of this creditors team has access to both register invoices and release them for payment. We understand that this is due to the fact that this person trains new members of staff in the recording of invoices. Although this training currently takes place in the live environment, we understand that it could be performed in the test environment that is available for Integra. This segregation of issues conflict applies to both the old and the new procurement through payables processes. <u>This condition poses the following risk(s) to the organisation</u>: a) Unauthorised invoices could be released for payment. b) Inadequate segregation of duties in the processing of supplier invoices.	Members of staff should not have simultaneous access to record invoices and to release them for payment in the Integra system. This segregation of duties conflict should be resolved with utmost priority. Any training in the input of supplier invoices should be performed in the test environment of Integra.	This access has now been removed and appropriate User Access has now been changed in the Live environment. All Training shall now be carried out in the Test Environment.

2	**Deficiency**	**Proactive Reviews of Logical Access within the network and applications**

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
User accounts and associated permissions within the network, Integra, Itrent and SQL server databases were not being formally, proactively reviewed for appropriateness. We understand that user access reviews at network and Itrent levels are intended to be performed in the near future. We noted a user account in the Integra system that has access to release invoices for payment. Although this account has not been used since 2012, the owner of this account no longer needs access to the Integra system. We understand that despite this access right, this member of staff could not access the Integra application as he is not a member of a specific group in Active Directory. We noted three users that had changed jobs during the last financial year. Despite this, these three users still have associated the old post references in Active Directory. Access rights in Active Directory are granted according to the associated post reference. We understand that these three job changes were not reported to the service desk. As a result of our review, we identified one user that had unnecessary access to the server running the Integra application. This user was member of the "support pansy", "support poppy" and "corp it development" groups in Active directory. This user	It is our experience that access privileges tend to accumulate over time. As such, there is a need for management to perform periodic, formal reviews of the user accounts and permissions within the network, Integra, Itrent and SQL server databases . These reviews should take place at a pre-defined, risk-based frequency (annually at a minimum) and should create an audit trail such that a third-party could determine when the reviews were performed, who was involved, and what access changed as a result. These reviews should evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with due consideration being given to adequate segregation of duties). We recommend that members of staff are reminded of their responsibility to report staff changes to the Service desk.	IT Services apply RBAC (Role Based Access Control) to restrict system access to authorised users. The user post number is supplied by HR with line managers defining the system access for that role. It's difficult for IT to challenge services on requested permissions due to a lack of understanding of individual business requirements, other than the most obvious anomalies. Agreed actions – 1. A sample audit of network permissions (2%) will be conducted each year and any anomalies addressed. 2. A daily script will be ran that compares the HR database and Active Directory that will highlight any mismatched posts/establishments/job titles and names to assist permission accuracy.

led the IT department in the past but she has moved jobs since then. We noted that membership of the "support pansy" and "corp IT development" groups was removed for this user as a result of our visit. <u>This condition poses the following risk(s) to the organisation</u>: a) Gaps in user administration processes and controls may not be identified and dealt with in a timely manner. b) Access to information resources and system functionality may not be restricted on the basis of legitimate business need. c) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls. d) No-longer-needed permissions may granted to end-users may lead to segregation of duties conflicts. e) Access privileges may become disproportionate with respect to end users' job duties.		A reminder email will be sent to line managers of the importance to report staff changes to Human resources in the first instance and then if appropriate onto the IT Service desk.

3	Deficiency	Disaster recovery

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The Council has its primary server room located in Midlothian House and a secondary one in Fairfield house. The distance between both locations is approximately 200 metres. Backup tapes are kept in a safe in the ground floor of Fairfield house. We understand that the Council is already aware of the potential implications that the proximity between both server rooms entails. We understand that there is an alternative location that could be confirmed within three to five years. The Council has duplicate IT capacity for the main applications split between both server rooms. Therefore, in the event of losing one server room, applications such as Integra (Finance) or Open Revenues (Council tax) could be run from the other server room. Additionally, the Council has produced a number of business continuity plans for the Integra, Itrent (Payroll) and Open Revenues applications among others. These plans detail different disaster scenarios and contain instructions to recover the applications in the event of a major issue affecting the IT infrastructure. The Council produced a test strategy for these business continuity plans covering IT infrastructure and applications. We understand that there has been a limited amount of	We recommend that the Council continues exploring the options to relocate the secondary server room and backup storage site to a more remote location. This location should provide adequate environmental and security conditions for hosting IT equipment and backup media. We recommend that the Council tests the recovery of the Open revenues and Integra systems at least on an annual basis Both the primary and secondary server rooms should be serviced by an electric generator as this would greatly assist the recovery of IT operations in the event of a power outage. We recommend that fire extinguishers are serviced in line with the Council's health and safety procedures. We recommend that the Council continues exploring the options to relocate the secondary server room and backup	The Contingency Planning Group are aware of this risk and as we move forward with our EWIM (property rationalisation) and new school build programme will explore and consider costed Business cases to mitigate this risk. To undertake this exercise currently in isolation of the wider council strategy is impractical at this time. Further opportunities may also be explored and considered as the National ICT Strategy evolves. The Council is continually working towards ensuring best practice in Business continuity and as highlighted have drawn up Business continuity test plans to support the main business critical systems. The two systems highlighted Open Revenues and Integra system will be prioritised as part of this process and it would be the Council's intention to carry out simulated Business continuity desk top exercises for these two systems over the coming year reporting the findings back to

business continuity testing in the last financial year. This testing included a test of the backup system and the NASA server, which hosts the fixed assets system. This limited testing was mainly due to the higher priority of the PSN compliance project that was recently completed. We also understand that there is an electric generator that covers the main server room at Midlothian house in the event of a power outage. However, there is no generator to cover the secondary server room in Fairfield house. There was a fire extinguisher in the Fairfield service room that was not serviced last year. We understand that management was going to fix it shortly after our visit. This condition poses the following risk(s) to the organisation: Given the proximity between the main and secondary server rooms, there is a risk that both rooms might be affected by a disaster. This issue might hamper the recovery of IT systems beyond a reasonable time. This could have a detrimental impact on Council services and lead to reputational damage.	storage site to a more remote location. We recommend that the Council tests the recovery of the Open revenues and Integra systems at least on an annual basis. Both the primary and secondary server rooms should be serviced by an electric generator as this would greatly assist the recovery of IT operations in the event of a power outage. We recommend that fire extinguishers are serviced in line with the Council's health and safety procedures – Complete.	the Contingency Planning group. Midlothian Council is currently in the process of procuring a Room UPS system for both Midlothian and Fairfield House – Server rooms. This newly procured solution (Room UPS) and proposed configuration will complement the existing standby generator with the main objective being to minimise any future power outage.

4	Deficiency	Information technology – Payment Card Industry – Data Security Standard (PCI-DSS)

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Credit card companies produced a security standard called PCI DSS to increase the security in transactions. The Council has proactively prepared a list of actions to comply with this standard. One of the outstanding actions detailed in this plan is the production of local secure card handling procedures. This condition poses the following risk(s) to the organisation: Members of staff could misuse credit card details resulting in fraudulent transactions, fines or negative publicity.	We recommend that the Council gives priority to the production of local secure card handling procedures as part of its efforts to comply with the PCI-DSS standard. The Council should allocate sufficient resources to implement the actions to comply with the PCI-DSS requirements.	The Council continues to work towards full PCI DSS compliance. An action plan has been produced and will be followed. Agreed Actions – Develop and issue a local secure card handling procedure to all those that process card payments

5	Deficiency	Reviews of Information Security Logs Created by Active Directory

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Logs of information security activity within Active Directory were not being formally, proactively, and routinely reviewed. We understand that this situation is due to insufficient resources. This condition poses the following risk(s) to the organisation: Without formal, proactive, and routine reviews of security event logs, inappropriate and anomalous security activity (e.g., repeated invalid login attempts, activity violating information security policies) may not identified and/or addressed in a timely manner.	Given the criticality of data accessible through Active Directory, logs of information security events (i.e., login activity, unauthorised access attempts, access provisioning activity) created by these systems should be proactively, formally reviewed for the purpose of detecting inappropriate or anomalous activity. These reviews should ideally be performed by one or more knowledgeable individuals who are independent of the day-to-day use or administration of these systems.	Although the security principle is accepted, the manual identification of anomalous behaviour via system logs is both technically challenging and resource intensive. Agreed Actions - Midlothian Council shall evaluate software products and processes that facilitate the review of audit logs and report findings back to the Digital Strategy Group for decision and prioritisation to mitigate this risk.