/

Midlothian

Chief Internal Auditor
Jill Stacey

Audit Committee
Tuesday 28 May 2019
Item No: 5.5

Auditor: James Polanski, Ext 5646

Internal Audit Report

to

Director, Resources
Head of Finance and Integrated Service Support
Digital Services Manager
Technical Service Delivery Manager
Information Governance / Security Services Lead
Waste, Risk and Civil Contingencies Manager

on

ICT Security Controls

26 April 2019

1 Introduction

1.1 The purpose of this audit was to review the framework in place to assess the adequacy of the physical access and environmental controls to ICT (Information Communication Technology) equipment, software and data to prevent unauthorised access / damage, including third party access and Public Services Network (PSN) compliance.

2 Audit Scope

2.1 The scope of the audit was to examine and evaluate the following areas:

- the structure and efficacy of arrangements and processes deployed in managing:
  - physical access and environmental monitoring;
  - disaster recovery procedures;
  - control of access by third parties; and
  - changes to the network.
- the efficacy of processes for identifying and managing non-compliance with policies and procedures in relation to the security of IT infrastructure.
- the processes for ensuring efficient compliance with the requirements of the Public Services Network (PSN) certification and with the Cyber Essentials certification regime.

3 Management Summary

3.1 ICT security controls are important to help mitigate the impact and reduce the likelihood of loss of information, disruption to services, damage to reputation, legal action, and potential costs of recovery. Implementing adequate business continuity and disaster recovery controls and procedures reduces business risk and the cost of recovery should an incident occur.

3.2 In order to participate in the PSN, organisations must undergo an annual external ICT security health check to test the adequacy of ICT security policies, systems, and controls. The Code of Connection requirements for accessing the PSN are stringent, and Midlothian Council is assessed against these requirements annually. The Cyber Essentials Plus certification is a voluntary programme the Council participates in, that demonstrates the Council's willingness to further improve its resilience against cyber-attacks. Midlothian's Digital Services team is dedicated to meeting the stringent security requirements from these external reviewers, and have advised audit that resources will continue to be directed towards this.

3.3 Midlothian Council has a wide range of comprehensive ICT security controls in place, including controls for physical access and monitoring, access by third parties, changes to the network, control of account permissions and active directory, patch management, anti-virus, firewall, internet filtering, and network monitoring. The Council once again achieved PSN compliance in 2018, and is on track to achieve this again in 2019.

3.4 Our audit did identify that 19 ICT business continuity plans had not been recently updated (*Recommendation 5.1*), and there was insufficient recent evidence of business continuity and disaster recovery testing (*Recommendation 5.2*). Management have advised audit that this in part reflects the direction of resources to maintaining the effectiveness of the security controls together with PSN accreditation. The Council's previous external auditors highlighted that only Midlothian House's server room has a backup generator but that there is no generator for Fairfield House, and the circumstances have not changed since their review (*Recommendation 5.3*).

3.5 A review of server room access identified 5 leavers who had not had their access disabled, and 12 current employees who did not require access to the server rooms (*Recommendation 5.5*). It was noted that although applications are in place for active directory security logs to be monitored and a robust audit trail of this is in place, there is currently limited proactive monitoring (*Recommendation 5.6*).

3.6 Some minor improvements could be made to ensure written procedures are in place for back office processes that were not fully documented (*Recommendation 5.4*), and consistent referencing for tracking PSN actions would make review of progress easier (*Recommendation 5.7*).

3.7 Internal Audit considers that the level of assurance we are able to give is **Substantial Assurance** in terms of the ICT Controls aspect of this review, and **Limited Assurance** for the disaster recovery and business continuity aspect.

3.8 The Internal Audit function conforms with the professional standards as set out in the Public Sector Internal Audit Standards (2017), including the production of this report to communicate the results of the review.

3.9 We would like to thank those officers who assisted us during our review.

4 Findings

Risk	Expected Control	Results	Effectiveness of Actual Control	Rec. Ref No
4.1 - ICT system failure, damage, or data loss, and resultant business continuity risks, reputational risks, and potential financial loss	Efficient and appropriately structured arrangements and processes in place for business continuity and disaster recovery	**Business Continuity Planning** Digital Services have created an overarching ICT Business Continuity Plan, and plans have been created for all key Council systems and for certain scenarios, such as a ransomware attack or the temporary loss of access to Midlothian House. The plans reviewed during the audit were well prepared and sufficiently detailed. Individual business continuity plans for each system have not been subject to regular review, relevant managers have not been informed of the plan, and of the results of any business continuity testing. Out of 40 plans sighted in the file directory, 19 had review dates before January 2014. There is a risk of errors occurring if there is an incident and the business continuity plans are not up to date, particularly if there are changes in staffing. There did not appear to be a plan in place covering total loss of a server room, e.g. through fire.	Partly Satisfactory	Rec 5.1
		Business Continuity Testing The Council's previous external auditors, Grant Thornton, recommended in 2012 that the Council should produce a test strategy for the IT business continuity plans. The document would detail the plans in scope, the disaster scenarios to be tested, and the frequency of the testing. This ICT Business Continuity Plans Testing Strategy was prepared by the Council's Digital Services team and presented to Audit Committee in 2013. Although for the first year the testing strategy was followed, in recent years the testing strategy has not been applied as originally intended. It has been advised that time spent testing business continuity procedures has been reduced due to resource constraints and other business as usual pressures with available resources focussed on maintaining the ICT security control arrangements and the increasingly stringent requirements to maintain PSN accreditation. This risk has been highlighted within the Digital Services risk register.	Unsatisfactory	Rec 5.2
		Server Room Locations and Backup Arrangements The Council has its primary server room located in Midlothian House and a secondary one in Fairfield House. Arrangements are in place to ensure that 6 weeks of data is backed up at these sites. A weekly backup of all the Council's data is held in a server room in the Lasswade Centre, and currently this holds 15 months of data. This offsite storage addresses	Satisfactory – system restores testing should be formalised	Rec 5.2

Risk	Expected Control	Results	Effectiveness of Actual Control	Rec. Ref No
		previous audit recommendations which raised issues on the basis of the close geographical location between Midlothian House and Fairfield House and all backups at the time being held there. Education servers are held at the Lasswade Centre, and on a weekly basis, and in addition to backup arrangements on site, the data is also backed up to tapes and these are held in Midlothian and Fairfield House. Digital Services have indicated that the tape drives used for Education backups is due for replacement in 2020, and may be replaced with a server hard disc solution. Whilst it is noted that system restores are carried out as required by Digital Services and evidence was demonstrated of this during the review, there is not a formal program for testing restores. **Backup Power for Server Rooms** The Midlothian House server room has a diesel powered backup electric generator. Fairfield House and the Lasswade Centre do not have a backup generator, they rely instead on batteries that may last up to an hour in the event of a power failure. Although it is understood that there is a cost to procuring and maintaining additional backup generators, having this in place would greatly assist the Council in recovering IT operations in the event of a power outage.	Unsatisfactory – ideally both server rooms should have adequate backup power	Rec 5.3
4.2 - Damage or loss of IT equipment, loss of data, reputational risks, and potential financial loss	Efficient and appropriately structured arrangements and processes in place for physical access and environmental monitoring; control of access by third parties; and changes to the network	**Policies and Procedures** Policies and procedures for ICT users are available on the Council's intranet. These were reviewed, along with some internal Digital Services procedures, such as the starters and leavers procedures and patch management policy and no issues were noted. Some Digital Services processes should be formally documented, such as the processes for identifying inactive accounts and mismatches, the approach taken for allocation of admin level active directory groupings, and some internal applications (e.g. internet filtering, firewall, anti-virus, and active directory auditing). **Control of Access by Third Parties** Controls have been established over the provision of access to third parties, such as suppliers. Suppliers may require some administrative privileges in order to fix issues. Suppliers have to formally request access	Satisfactory – gaps identified should be addressed. Good	Rec 5.4 -

Risk	Expected Control	Results	Effectiveness of Actual Control	Rec. Ref No
		by submitting a form to Digital Services, and authorisation for this must be sought. Access is limited to only what is necessary, for example, If a supplier only needs to do work on the server, not the desktop PCs, they are only given administrative access to necessary servers and not given desktop admin access. Suppliers are given an account that only lasts for 1 day, and a new form needs to be submitted for any additional access. A sample of access requests were reviewed and no issues were noted. **Changes to the Network** Significant changes to the network (eg installation of new equipment) or configuration changes to firewall settings require a documented Request for Change Approval form to be prepared and approved by management in Digital Services. This process helps ensure that there is an audit trail of any significant changes, and segregation of duties in terms of the request, the approval of the request, monitoring, and the implementation of the request. **Physical Access and Environmental Monitoring** Physical access to the Fairfield and Midlothian House server rooms is controlled through the Midlothian card entry system, and this is managed by Business Support. Access to the Lasswade server room is via a locked door with the keys held by Digital Services and at the centre. Leavers' reports are received for access to be revoked as required. A review of physical access reports for the server rooms identified 5 leavers that still had access, and 12 employees who do not require access to these rooms (but this may be increased now that management have reviewed the audit findings). CCTV is in place for all server rooms, and a room monitoring system is in place to monitor temperature and humidity. Alerts are in place if the temperature or humidity increases beyond set levels in the system, and an out of hours service is in place with East Lothian Council to ensure the condition of the room is continually monitored.	Good Partly Satisfactory – Digital Services need to periodically review the list of employees with access to the Council's server rooms.	- Rec 5.5
4.3 - Council's ICT information and assets are put at risk due to undetected non-compliance with	The efficacy of processes for identifying and managing non-compliance with policies and procedures	**Access Controls and Active Directory Audit** A system is in place to allow all individual accounts within the Active Directory (AD) to be audited. This includes details of changes to all AD users and groups, all files opened, deleted, modified, and moved by users. This log is maintained for 180 days. A review of AD Groupings noted that they appear to be appropriate. However, best practice would be to outline	Satisfactory – robust audit trail and appropriate access	Rec 5.4 and Rec 5.6

Risk	Expected Control	Results	Effectiveness of Actual Control	Rec. Ref No
established policies and procedures	in relation to the security of IT infrastructure	in an approved procedure the decisions taken in the allocation of users to AD groupings with administrative privileges. Processes have been established for file access permissions to be segregated by directorate and team in the Council structure, and for changes to be approved by a relevant manager with oversight from Digital Services. However, there is no proactive monitoring of security logs generated by Active Directory, or sample testing of permissions granted to users. It has been advised that monitoring and testing as described above is resource intensive, and business as usual activities have taken priority over this. Insufficient review of logs is an issue that has previously been raised by the Council's External Auditors (2014 External Audit Report). **Patch Management** A patch management policy is in place for Digital Services, as was evidence of application of the policy. PSN have reported positively on Digital Service's patch management. **Anti-Virus** Appropriate anti-virus software is installed on Council ICT devices and processes are in place to ensure virus definitions are regularly updated and scans undertaken. It was noted that alerts have been established using the Council's anti-virus software for all data leaving the Council, e.g. on USB devices. **Firewall** Perimeter firewalls are in place, along with a backups in case a firewall fails and procedures are in place to check the firewalls are operational. PSN review the rule base annually, and have reported positively on this. The existing firewalls are reaching the end of their useful life and do not have the advanced functionality available in some modern firewalls, such as Intrusion Prevention Systems (IPS) or Intrusion Detection Systems. Such systems allow more effective, targeted, monitoring of logs, and allow additional scanning of data for malware and viruses before the data reaches the Council's trusted network. A new firewall with an IPS is currently being trialled by Digital Services.	groupings, but no proactive monitoring. Good Good Satisfactory	- - -

Risk	Expected Control	Results	Effectiveness of Actual Control	Rec. Ref No
		Internet Filtering Appropriate internet filtering systems are in place for both the Corporate and Education networks, adequate rules have been established for these systems, and processes established to take backups of the device configuration. Additional monitoring and alerts are in place for the Education network as part of the Council's safeguarding role. For the Corporate network, suitable reports can be made available to managers on request. **Monitoring Processes - Network** Network monitoring software is in place for the Corporate Network. As well as providing basic monitoring of the efficiency of devices and that devices are connected, it can back-up the configuration of key network devices. The Council has Security Information and Event Management software installed for the Corporate network; the licence for this was renewed in December 2018 and further training on this was provided by the supplier. This monitoring software allows comprehensive monitoring of servers, exchange (email system), Domain Name Services, Dynamic Host Configuration Protocols, and Security Logs. Further monitoring of changes to applications is planned to be rolled out for 2019 using this application, and monitoring procedures established.	Good Satisfactory – further rollout of monitoring planned for 2019	- -
4.4 - Loss of privileges to interact appropriately with PSN due to failure to maintain the certification (eg to allow the Council to access benefits data from DWP) and resultant reputational and security risks	Processes for ensuring efficient compliance with the requirements of the Public Services Network (PSN) certification and with the Government's Cyber Essentials (CSE) certification regime are in place	**PSN and CSE Compliance** The Council has achieved PSN accreditation each year, and is on track to receive accreditation for 2019. The PSN findings for the 2019 review were discussed with relevant Digital Services employees, and it was noted that the majority of findings raised this year are low risk, with the majority of the remaining medium risk findings being outstanding for a justifiable reason (e.g. to address would cause issues with a business critical system, or is an issue that will be addressed by the Council's transition to Windows 10). It was noted that the PSN remediation plan for 2018 did not use the same recommendation reference code as the PSN report. In future it would be helpful to use the same referencing so it is easier to track progress on each PSN finding.	Good – tracking of specific actions could be improved	Rec 5.7

5 Recommendations

Rec. Ref No	Recommendation	Rating	Management Response	Responsibility and Timescale
5.1	All Business Continuity Plans should be subject to periodic review, and business owners to be periodically informed of the plans and results of any testing. Plans should include response to significant damage to Digital Services, e.g. from vandalism or fire.	Medium	The Council's Risk and Resilience group are aware of the current position and Digital Services' resources are having to be prioritised in line with the core strategic projects identified across the Council. To mitigate part of this action, Digital Services have made a case to secure a Cyber Security Engineer and have approval to start the recruitment process. Recruitment to this new role will help to put in place improved governance and testing of Business continuity plans along with the Cybersecurity controls expected to be in place as part of the Scottish Government Cyber security actions plan. Action – recruitment to Cyber Security post	Digital Services Manager by 30/09/2019
5.2	Digital Services should update and review their testing strategy for the IT business continuity plans. This document should detail the plans in scope, the disaster scenarios to be tested, testing of system restores, and the frequency for this test. The testing strategy should be periodically reported on to relevant Management.	Medium	See supporting statement above 5.2 in relation to resource and new position. Digital Services, subject to the caveats highlighted above, would intend to implement an incremental testing strategy focusing on high priority systems given the amount of resource required to be committed for specific business testing scenarios. Digital Services are also considering undertaking Desktop Exercises on priority systems which will help to review existing documentation, processes, procedures and then evidence the findings from the exercises. Action – recruitment to Cyber Security post	Digital Services Manager by 30/09/2019
5.3	Management should again review the feasibility and business case for having both Midlothian and Fairfield server rooms serviced by backup generators, taking into account the wider Council Strategic Property Programme.	Medium	The Councils Risk and Resilience group are aware of the current arrangements in relation to back-up generators between Midlothian and Fairfield house and the degree of risk associated with this. To again review the feasibility and business case in isolation is impractical and will add no value. Opportunities to review server room provision will be considered as part of the wider Council strategic	No specific actions proposed

Rec. Ref No	Recommendation	Rating	Management Response	Responsibility and Timescale
			property programme and the implications as Council shifts to systems being increasingly hosted.	
5.4	Internal processes and monitoring controls as noted in the report should be documented in written procedures approved by Management.	Low	Digital Services shall look to update its internal processes and monitoring controls with updated and refreshed procedures based on the areas identified in the audit Action – A workplan will be in put in place by the timescale indicated to deliver this	Digital Services Manager by 30/09/2019
5.5	Digital Services should regularly review who has access to all of the Council's server rooms.	Medium	Digital Services will now request a routine User Door access report from Business Services team and will compare this to the leavers report. Action – recommendation to be implemented	Digital Services Manager by 30/06/2019
5.6	Management should review the resource allocated for proactive monitoring of active directory security logs, and testing of file and system permissions on a sample basis (e.g. 2%).	Medium	Digital Services have procured a Security Information and Event Management (SIEM) application to assist in the monitoring of security logs and testing file and system. This is a fairly resource intensive activity and needs to be balanced against all other Council priorities and available resources. The appointment of the new Cybersecurity post and their associated duties will be to sample these logs and report any concerns to DS management team. Digital Services will target key systems with the nominated System administrator on an annual basis to review active directory, applications and database permissions and then evidence the findings from this exercise. Action – new working arrangements will be agreed and put in place by the date indicated	Digital Services Manager by 30/09/2019
5.7	The same referencing for recommendations from the PSN report should be used in the PSN remediation plan to make it easier to track progress on PSN findings.	Low	Digital Services on the basis of this recommendation shall use the same referencing so it is easier to track progress on each PSN finding \ action in the future. Action – this will be reflected in the 2019 PSN action plan	Digital Services Manager by 30/06/2019

Overall Audit Opinion level and definition

Comprehensive Assurance	Sound risk, control, and governance systems are in place. These should be effective in mitigating risks to the achievement of objectives. Some improvements in a few, relatively minor, areas might be required.
Substantial Assurance	Largely satisfactory risk, control, and governance systems are in place. There is, however, some scope for improvement as current arrangements could undermine the achievement of objectives or leave them vulnerable to error or misuse.
Limited Assurance	Risk, control, and governance systems have some satisfactory aspects. There are, however, some significant weaknesses likely to undermine the achievement of objectives and leave them vulnerable to an unacceptable risk of error or misuse.
No Assurance	The systems for risk, control, and governance are ineffectively designed and operated. Objectives are not being achieved and the risk of serious error or misuse is unacceptable. Significant improvements are required.

Recommendation Ratings

Recommendations in Internal Audit Reports are suggested changes to existing procedures or processes, to improve the controls or to introduce controls where none exist. The rating of each recommendation reflects our risk assessment of non-implementation, being the product of the likelihood of the risk materialising and its impact. The ratings are:

High	Significant weaknesses in existing controls, leaving the Council or Service open to error, fraud, financial loss or reputational damage, where the risk is sufficiently high to require immediate action within one month of formally raising the issue. The risk should be added by Management to the relevant Risk Register for control and monitoring purposes and included in the relevant Head of Service Annual Assurance Statement.
Medium	Substantial weaknesses in existing controls, leaving the Council or Service open to medium risk of error, fraud, financial loss or reputational damage requiring reasonably urgent action within three months of formally raising the issue.
Low	Moderate weaknesses in existing controls, leaving the Council or Service open to low risk of error, fraud, financial loss or reputational damage requiring action within six months of formally raising the issue to improve efficiency, effectiveness and economy of operations or which otherwise require to be brought to the attention of Senior Management.
Other	Minor administrative weaknesses posing little risk of error, fraud, financial loss or reputational damage.

The Action Plans in Internal Audit Reports address only Recommendations rated High, Medium or Low. Outwith the Internal Audit Report, we inform Service Management about Other Minor matters to improve internal control and governance.

The recommendations will be input to Pentana performance system to assist with Management tracking of implementation. If responsible owners are unable to achieve the standard timescales for actions please notify the Chief Internal Auditor with the reason for the delay in implementation and the revised timescales to assist with the implementation and follow-up of these recommendations to improve internal control and governance.

Jill Stacey
Chief Internal Auditor