CITY OF GLASGOW COLLEGE

Board of Management

Audit Committee

Date of Meeting	**Wednesday 13 September 2017**
Paper No.	**AC1-H**
Agenda Item	**8.4**
Subject of Paper	**Internal Audit Report – IT Network Arrangements/Security**
FOISA Status	**Disclosable**
Primary Contact	**Henderson Loggie**
Date of production	**August 2017**
Action	**For Discussion and Decision**

Recommendations

The Committee is asked to consider and discuss the report and the management responses to the internal audit recommendations.

1. Purpose of report

The purpose of this review is to provide management and the Audit Committee with assurance on key controls relating to the curriculum and financial plans in place for City of Glasgow College and their alignment with the regional plan for Glasgow and the college student number targets.

2. Context and Discussion

Following the Audit Needs Assessment undertaken by Henderson Loggie in session 2016-17, and the consequent Internal Audit Strategic Plan 2016-2020, both approved by the Committee in March 2017, an operating plan was created for the year ended 31 July 2017.

This internal audit of IT Network Arrangements/Security provides an outline of the objectives, scope, findings and graded recommendations as appropriate, together with management responses. This constitutes an action pan for improvement.

The Report includes a number of audit findings which are assessed and graded to denote the overall level of assurance that can be taken from the Report. The gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

3. Impact and implications

Refer to internal audit report.

HENDERSON LOGGIE
Chartered Accountants

City of Glasgow College

IT Network Arrangements / Security

Internal Audit Report No: 2017/06

Draft Issued: 30 June 2017

Final Issued: 7 August 2017

LEVEL OF ASSURANCE	Satisfactory

Content

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires Improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the College to material risk and which requires to be brought to the attention of the Audit Committee.
Priority 2	Issue subjecting the College to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the College to minor risk or which, if addressed, will enhance efficiency and effectiveness.

1. Overall Level of Assurance

Satisfactory	System meets control objectives with some weaknesses present.

2. Risk Assessment

This review focussed on the controls in place to mitigate the following risks included on the City of Glasgow College (‘the College’) Risk Register:

- Growth and Development: Failure to achieve New Campus objectives (net risk score 5);
- Growth and Development: Negative impact upon College reputation (net risk score 10); and
- Process and Performance: Failure of Business Continuity (net risk score 12).

3. Background

As part of the Internal Audit programme at the College for 2016/17 we carried out a review of the IT network arrangements / security, with a focus on the IT infrastructure. The Audit Needs Assessment, completed in March 2017, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Board of Management and the Principal that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

Network architecture and design is the responsibility of the Network Team. The Network Team is led by the Head of IT Infrastructure who reports to the Vice Principal, Infrastructure. In addition to architecture and design, the Network Team is also responsible for maintaining and monitoring the network infrastructure to ensure that network services are available, provide adequate performance and are secure for all users. The Network Team also administers network level security such as firewalls, routers and intrusion prevention systems to protect the College’s information systems and users from cybersecurity threats originating from the Internet. The College network covers two main locations, the Riverside Campus, which opened in August 2015 and the City Campus, which opened in August 2016.

4. Scope, Objectives and Overall Findings

This audit assessed the College's network architecture and design from a security perspective to determine whether adequate security mechanisms are in place and operating effectively.

Our review encompassed the design and configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures that provide guidance on how network security should be managed by both the IT department and users.

The table below notes each separate objective for this review and records the results:

Objective	Findings				
The objective of this audit was to obtain reasonable assurance that:	**Assurance**	**1**	**2**	**3**	**Actions already planned**
		No. of Agreed Actions			
1. The network architecture is appropriately designed to provide security and resilience, including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices.	**Satisfactory**	0	0	3	✓
2. Robust procedures are in place regarding configuration (hardening) of network devices and user and administrative access to network services and devices.	**Good**	0	0	0	✓
3. Remote access to the corporate internal network is appropriately controlled.	**Good**	0	0	0	
4. Logging and monitoring of network devices, including periodic firewall rule reviews, is performed.	**Satisfactory**	0	0	2	
5. There are physical controls over access to critical network hardware and cabling.	**Good**	0	0	0	
Overall Level of Assurance	**Satisfactory**	**0**	**0**	**5**	
		System meets control objectives with some weaknesses present.			

5. Audit Approach

Our approach was based upon the guidance and best practice provided by ISACA (previously known as the Information Systems Audit and Control Association), discussion with the Vice Principal, Infrastructure, Head of IT Infrastructure and other members of the IT Team, review of relevant documentation; and observation.

6. Summary of Main Findings

Strengths

- Overall, we found that the network is operating well, serving the needs of the College and no significant deficiencies in its architecture or design were noted. In particular, there is ample capacity for current needs and peak demands, and there is an on-going effort to improve performance and reduce costs. The Network Team was found to be knowledgeable and committed to process improvement.
- The College network environment is protected by a suite of Cisco firewall appliances and subject to both internal and external penetration testing. Sophos anti-virus software is deployed at the network and end user level, incorporating on-access scanning plus scanning of email and internet access. An intrusion prevention system (IPS) is installed at the network perimeter which would identify, log, block and report any malicious network activity.

Weaknesses

- IT infrastructure development actions have been identified, albeit informally, and these should be fully documented to adequately identify tasks, allow appropriate prioritisation based on risk and available resources and allow tracking to completion. Development of an IT operational risk register would assist the IT Team in this regard.
- Although the College has an IT Acceptable Use Policy in place, the College's Information Security Policy Set and supporting processes and procedures is incomplete in terms of the operational documents included in good practice produced by ISACA and other IT governance bodies. Furthermore, there are no defined processes or procedures which govern the management of the IT infrastructure or use of IT services. Instead there is a reliance on the knowledge and experience of the current IT Team members.
- During our review, we noted that the IT Team comprises knowledgeable and experienced staff, however we also identified that in some areas the IT Team relies heavily on the knowledge and expertise of particular members of staff. This represents a vulnerability in terms of business continuity. We recommend that the College considers how resilience can be developed by way of knowledge transfer across the IT Team.
- We noted that the members of the IT Team meet regularly to discuss any issues that affect the IT network and infrastructure and work collaboratively to address these. However, this is largely done informally and there are no formal change management procedures that detail how changes are identified, who can approve changes, the staff that have overall responsibility for change management and how emergency changes are managed and approved.

7. Acknowledgements

We would like to thank the College staff for the co-operation and assistance we received during the course of our review

8. Findings and Action Plan

Objective 1: The network architecture is appropriately designed to provide security and resilience, including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices

Overall, we found that the network is operating well, serving the needs of the College and no significant deficiencies in its architecture or design were noted. In particular, there is ample capacity for current needs and peak demands, and there is an on-going effort to improve performance and reduce costs. The Network Team was found to be knowledgeable and committed to process improvement.

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources.

The College's network is documented and described in a series of network design documents which include topology diagrams.

Our review of the network infrastructure confirmed the following:

- the network environment is protected by internal and external Cisco firewall appliances. Firewalls are configured to capture and record activities including: log-in attempt success and failure; administrator activities performed; and changes to firewall configuration;
- appropriate use of DMZs, a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet, was found to be incorporated into the network design;
- we found through a high-level review of firewall rules that IP addresses, which define communication permissions in and out of the network and across the network, were appropriate; and
- routers, which are used to define paths between networks and securely transmit information across those paths toward an intended destination, were found to be located at key points on the network.

User access to the Internet via the network is restricted via the use of firewall and proxy servers. In order to minimise risks around staff access to high risk Internet sites and malicious software being introduced into the network through web site access, all Internet access is filtered and access to unsuitable sites blocked accordingly.

Objective 1: The network architecture is appropriately designed to provide security and resilience, including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices (Continued)

Internet gateway controls include:

- perimeter located SPAM detection is used to reduce the risk of virus infected e-mails reaching the College's e-mail server;
- anti-virus solutions are used to scan inbound e-mail traffic; and
- penetration testing is undertaken by a third party in order to identify weaknesses in the security of the network perimeter.

The College has adopted a multi-layered approach to anti-virus and malware prevention and detection, with virus protection controls being deployed at the Internet / network gateway level, at the network / server level and on individual laptop and desktop machines.

College laptop and tablet computers have disk encryption implemented using Microsoft 'Bitlocker' encryption. This ensures that data cannot be accessed on mobile computers without appropriate credentials, restricting access to data on the machine and minimising the risk of unauthorised access to the network in the event of the loss or theft of the machine.

Use of unauthorised USB devices is not currently restricted; however devices are scanned when connected to the network using the Sophos 'Endpoint' system. In order to address the risk of data loss the College is currently considering restricting USB access by default or issuing secure USBs to staff and as such we have not raised a recommendation at this time.

All servers are backed-up by the Infrastructure Team to mitigate the risk of a virus infection. Desktop and laptops are protected against malware via the use of Sophos. Automatic updating of virus definitions and updates is enabled to ensure machines are protected from the latest threats.

Access to the College network is provided to users through the creation of an Active Directory account. By default, users are assigned the minimum levels of access required to perform their role. This includes the provision of domain membership, application of standard desktop configuration policies and access to the Internet. This minimum level of access can be upgraded at the discretion of a user's line manager, who is able to request that the user's access be matched to an existing group profile which determines permission levels.

User access requests are sent to the service desk in the form of an email from a senior, approved member of staff and / or Human Resources. This email incudes detail on the access levels that the user requires and acts as the authorisation needed to create or change users' access permissions. The information provided in the email is then actioned by IT staff.

Objective 1: The network architecture is appropriately designed to provide security and resilience, including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices (Continued)

Observation	Risk	Recommendation	Management Response	
The College network was principally designed by Glasgow Learning Quarter (GLQ), the special purpose vehicle set up to deliver the College campuses, however the College's IT Team had significant input into this process during the campus build to ensure that the project was delivered as intended. Since the City Campus opened in August 2016 the IT Team resource has focussed on addressing minor implementation issues, with little time allocated to network development. During our review, we noted that the IT Team has identified a number of development actions, however these have been assigned to individual members of the team on an informal basis. Actions should be fully documented to adequately identify tasks, allow appropriate prioritisation based on risk and available resources and to allow tracking to completion. Additionally, we noted that the IT Team has not produced an IT operational risk register that clearly identifies the network vulnerabilities, single points of failure and security weaknesses. A risk register should be used to determine the College's exposure, risk assess each issue and identify prioritisation of risks to be addressed.	Actions are not prioritised, resulting in inappropriate allocation of resources, which may result in tasks that would achieve the highest impact, and therefore add the most value, not being undertaken first, or areas of significant risk not being addressed timeously.	**R1** The IT Team should develop an action plan that identifies required IT network development work. This process should naturally cover what is achievable given the current IT resources, therefore any current resource constraints could then be identified and managed at that point.	The College will compile an action plan for the network highlighting any development work and resources required for the forthcoming year. **To be actioned by:** Head of Service **No later than:** 31 December 2017	
			Grade	3
		R2 Undertake an IT risk assessment and formally record identified vulnerabilities in the form of an IT operational risk register. The register should then inform the prioritisation of IT tasks at **R1**.	The College is compiling a Disaster Recovery document which will identify and record risks and vulnerabilities in the installed infrastructure. **To be actioned by:** Heads of Service **No later than:** 31 October 2017	
			Grade	3

Objective 1: The network architecture is appropriately designed to provide security and resilience, including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices (Continued)

Observation	Risk	Recommendation	Management Response	
Although the College has an IT Acceptable Use Policy in place, the College's Information Security Policy Set and supporting processes and procedures is incomplete in terms of the operational documents included in good practice produced by ISACA and other IT governance bodies. Details of the types of policies that should be included have been discussed with the IT Team, for example, Firewall Policy and Third-Party Access Policy. Furthermore, there are no defined processes or procedures which govern the management of the IT infrastructure or use of IT services, instead there is a reliance on the knowledge and experience of the current IT Team members. The IT Team is aware of the need to develop a comprehensive Information Security Policy Set, but due to competing pressures on IT staff resource this has not been progressed.	Users in general are not directed to perform activities in a secure manner and the IT Team has no documentation to guide the activities it undertakes. Both expose the College to additional risk.	**R3** Create a comprehensive Information Security Policy Set that addresses the way that the College IT Team intends to operate. This should also include documenting supporting IT processes and procedures so that the Information Security Policy Set can be implemented appropriately.	The College is updating and reviewing security and IT policies thus enabling the current documents to match the installed infrastructure and services. **To be actioned by:** Network Development Manager **No later than:** 31 October 2017	
			Grade	**3**

Objective 2: Robust procedures are in place regarding configuration (hardening) of network devices and user and administrative access to network services and devices

Our review identified that although a register of IT assets is held, a network discovery exercise had not been undertaken at the time of our fieldwork in order to identify devices connected to the network and their characteristics such as operating system, open ports, listening network services, etc.

It is possible to reset the counters on switches, which connect multiple PCs, printers, servers and other networked hardware and allow users to send information across the network in a controlled manner. This would allow the IT Team to identify the internal port and IP addresses of devices communicating across the network that are active or inactive.

In addition, access control lists (ACLs) can be implemented to harden the network even further (ACLs are a network filter utilised by routers and some switches to permit and restrict data flows into and out of network interfaces). When an ACL is configured on an interface, the network device analyses data passing through the interface, compares it to the criteria described in the ACL, and either permits the data to flow or prohibits it.

A combination of counter resets and review of ACLs would be one way to ensure that all devices that are connected are necessary and those that are not can be identified and disconnected.

At the time of our review the Network Development Manager had recently prepared an internal discussion paper which outlined proposals for infrastructure development and network security hardening, including how ACLs should be configured. Our review of the discussion paper noted that the proposals would adequately address the issues noted above in terms of device identification, communication between devices and network hardening. We have since obtained confirmation from management that the proposals have been agreed and an action plan developed to take the proposals forward. A number of these actions have now been implemented, including restricting how devices communicate across different segments of the network.

Objective 3: Remote access to the corporate internal network is appropriately controlled

The College uses a Citrix desktop solution, which allows users remote access to College data and applications via a virtual desktop environment without accessing the Active Directory database directly. The IT Team has configured the application to ensure that College data accessed remotely via Citrix cannot be saved down onto the users own device, thereby reducing the risk of data loss.

Access to the Citrix remote desktop application and other systems is governed by user accounts listed in Active Directory which means that when a member of staff or a student leaves the College their Active Directory account is disabled, which in turns disables access to all systems.

The College has procedures and controls in place which ensure that when an employee leaves or changes their employment, their access rights to IT services are immediately reviewed and appropriate action is promptly taken. This process is driven by Human Resources for staff users and Student Services for student users, who notify the IT Team of any changes. The College periodically performs a review of user accounts to ensure that user functionality is appropriate. IT staff assign new users to student or staff group profiles, with permissions based on systems access requirements or job role.

Objective 4: Logging and monitoring of network devices, including periodic firewall rule reviews, is performed

Audit logs of activity on devices and the network that connects them have been established. However, due to the resource required, these are not reviewed as a matter of course. Instead the IT Team has adopted a holistic approach to network monitoring which focuses on monitoring unusual activity, device load and capacity and utilises system alerts to notify IT staff of any risks or issues. A dashboard system has been developed to aid IT staff in this regard. We are satisfied that the approach taken by the IT Team is appropriate.

An Intrusion Prevention System (IPS) is deployed on perimeter firewalls and reports are reviewed daily to identify:

- unauthorised connection attempts
- outbound activity from internal servers
- IP addresses that are rejected
- source routed packets (which can be used to gain access to a PC or other network enabled device that is exposed to the Internet)
- load on the firewall
- rule changes
- unusual IP addresses trying to communicate with the College network.

Firewall activity reports and firewall rules are reviewed weekly by a member of the IT Team. As previously stated under Objective 1 we performed a high-level review of firewall rules and concluded that these were appropriate.

Objective 4: Logging and monitoring of network devices, including periodic firewall rule reviews, is performed (Continued)

Observation	Risk	Recommendation	Management Response	
During our review, we noted that the IT Team comprises knowledgeable and experienced staff, however we also identified that in some areas the IT Team relies heavily on the knowledge and expertise of particular members of staff. For example, a single member of the IT Team is responsible for all aspects of the firewalls including the configuration and review of the firewall rule sets.	Reliance on the knowledge and expertise of specific staff in key areas where there is limited knowledge transfer undertaken between IT staff represents a vulnerability in terms of business continuity.	**R4** As part of the development of an IT operational risk register (**R2**) identify where the IT Team relies heavily on the knowledge and experience of specific members of IT staff and consider how resilience can be developed by way of knowledge transfer across the IT Team.	College will arrange knowledge transfer sessions between members of staff in order that risk may be reduced. The College has also permanently appointed the temporary Telecoms Officer to ensure that this key skill is not lost. **To be actioned by:** Head of Service **No later than:** 30 November 2017	
			Grade	**3**

Objective 4: Logging and monitoring of network devices, including periodic firewall rule reviews, is performed (Continued)

IT change management is the controlled process for managing system changes within IT to help ensure that changes are formally evaluated, tested and implemented in a controlled manner so that they are applied in a consistent manner across IT systems. This helps to ensure that risks relating to system changes are mitigated to avoid conflict occurring within the existing IT environment. Creating comprehensive change management procedures helps to ensure that staff are fully aware of the change management process. This also provides guidance on how change management should be implemented within the College and defines the expected standards of how IT change should be implemented.

Observation	Risk	Recommendation	Management Response
We noted that members of the IT Team meet regularly to discuss any issues which affect the IT network and infrastructure and work collaboratively to address these. However, this is largely done informally and there are no formal change management procedures which detail how changes are identified, who can approve changes, the staff that have overall responsibility for change management and how emergency changes are managed and approved. Good practice in change management recognised by ISACA under the COBIT 5 assurance framework recommends that an appropriate group is established to review and approve changes to the IT infrastructure and network.	Where change management procedures are not in place there is an increased risk that changes to the IT infrastructure are not managed according to specific processes and that changes may not be adequately tested or authorised prior to implementation.	**R5** Ensure that a comprehensive change management procedure is documented to outline all stages of the IT change management process. The procedure should include forming a change control board or group comprising senior members of the IT Team which meets weekly, and contain information regarding the processes and responsibilities for change identification, the approval process and the emergency change process.	The College will form a change management committee and will formally document and agree changes to infrastructure that will be actioned during appropriate service maintenance windows. **To be actioned by:** Head of Service **No later than:** 30 November 2017 **Grade** 3

Objective 5: There are physical controls over access to critical network hardware and cabling

Access to the College's server and communications rooms at both campuses are gained through the use of smart access cards which are configured and issued by the IT Team. Cards are issued to all staff however only IT and Estates staff, and members of the Senior Management Team, are authorised to access areas that house critical IT equipment. GLQ personnel have also been issued with access cards, which are closely monitored by the IT Team as part of regular reviews of smart card access logs for server and communications rooms.

Inspection of one of the communications rooms within the student residences block at the Riverside Campus noted that IT equipment in the cabinet was being powered via a cable plugged into a wall socket instead of being hard cabled or power lined into the mains at the rear of the cabinet (i.e. protected from accidental or deliberate power down). There was evidence that the room was also being used by GLQ personnel and so there was an increased risk of power to the equipment being lost or interrupted if GLQ personnel were to accidently switch off the socket or use the socket for their own equipment without having any real understanding of what was being powered. We have since obtained confirmation from management that the IT Team has ensured that power cabling in the room is adequately protected by connecting the power into the mains at the rear of the cabinet.