ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	25 September 2019
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2005 – Cyber Security
REPORT NUMBER	IA/AC2005
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on Cyber Security.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of Cyber Security.

3.2 Management Comments

3.2.1 The increasing use of digital technology brings many benefits to our organisation, however there is a constant and ever-changing threat landscape. This audit has been a supportive and useful measure and provides reassurance to both the IT Security team and the wider business of our awareness and positive approach to protect the organisation against cyber threats.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC2005 – Cyber Security.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

Internal Audit Report

Digital & Technology

Cyber Security

Issued to:
Andy McDonald, Director of Customer Services
Andrew Howe, Chief Officer – Digital and Technology
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
Norman Hogg, Security Architect
External Audit

Date of Issue: August 2019 **Report No. AC2005**

EXECUTIVE SUMMARY

The Council's Corporate Risk Register identifies Cyber Threats as a risk to the Council's core functions and data. It details a number of mitigating controls that are in place to manage this threat and the objective of this audit was to provide assurance over these controls.

Risk Registers in place contain appropriate risk assessments and mitigating controls which take cognisance of national guidance. Where controls are not considered by management to be fully effective, an assurance action has been put in place to make necessary improvements.

Whilst progress with Cyber Security assurance actions had been reported regularly as expected, some actions had been delayed. Assurance actions were found to be progressing as expected towards revised due dates reported, with the exception of one action to risk assess Council systems for criticality, which will require further action upon the release of the Scottish Government Cyber Resilience Framework by the Scottish Government.

The Service is reporting regularly on Cyber Security breaches and their related prevention, to the Digital and Technology Management Team, Information Governance Group, and Audit, Risk and Scrutiny Committee.

Work has been undertaken to address the elements of key actions in the Cyber Resilience Scottish Government's Public Sector Action Plan which the Council is responsible for.

The Council was carrying out IT Health Checks annually and demonstrated compliance with the Payment Card Industry Data Security Standard required to take card payments. The Council has yet to obtain Public Sector Network accreditation, required to facilitate collaboration with public sector organisations. This is due to be reassessed following the next ITHC in August 2019.

Some minor issues were identified during testing and, following discussion as detailed in the main section of this report, were addressed by the Service.

1. INTRODUCTION

1.1 The National Cyber Security Strategy describes 'cyber security' as: "the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures." Cyber resilience is key for Council infrastructure, systems and data to remain secure and effective.

1.2 The Scottish Government issued a Cyber Resilience Strategy Public Sector Action Plan 2017/18 with a number of key actions for all Scottish public bodies, with the aim that they work towards becoming exemplars in respect of cyber resilience, being well on their way to achieving this by the end of 2018.

1.3 In the twelve months to 30 June 2019 there were 20,532,717 incident attempts, 10 of which were successful and all were mitigated. In comparison, in the twelve months to 30 June 2018 there were 40,790,746 incident attempts, 12 of which were successful, and all were mitigated.

1.4 The objective of this audit was to provide assurance that the controls detailed in the Corporate Risk Register (CRR) under Corp006 – Cyber Security are effective and that Assurance Actions are progressing as planned.

1.5 Corp006 is defined as "Cyber Threats must be mitigated to protect the Council, its essential functions and customer data" and identifies a number of risk impacts, such as service disruption and reputational damage; causes, such as human error and failure to identify cyber threats; and controls, such as password security controls and staff training.

1.6 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Andrew Howe, Chief Officer – Digital and Technology, and Norman Hogg, Security Architect.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Policies and Procedures

2.1.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff. This is important in the event of an experienced employee being absent or leaving, and they have increased importance where new systems or procedures are being introduced.

2.1.2 Written procedures and guidance covering cyber security, risk assessment and risk reporting are available on the Zone, primarily on the Introduction to Information Security page. These include the Risk Management Framework, the Corporate Information Policy, the Protective Monitoring Policy, the ICT Acceptable Use Policy and ICT Access Control Policy, the Managing Information Handbook and a guide to Information Security Incident Reporting.

2.1.3 The policies were reviewed and they were considered to be comprehensive and up to date; all had been reviewed as scheduled. One guidance document, Internet & Email FAQs, did not contain version dates and contained obsolete information; the Service advised that this has been replaced by the Protective Monitoring Policy and associated documents and should have been removed from the Zone when these were published. This has now been done.

2.2 Training

2.2.1 The Scottish Government Public Sector Action Plan key action 6 requires public bodies to provide assurances on appropriate staff training, awareness raising, and disciplinary policies with regard to cyber resilience. Expected standards of behaviour are covered in the Employee Code of Conduct, which states “Employees are required to always do their best in their jobs and to always act to protect the interests of the Council. Employees are expected to carry out all proper instructions and observe the rules, policies and procedures laid down to ensure efficient working and to secure the safety of themselves and others”. The Code of Conduct refers to the ICT Acceptable Use Policy, which details what use is not acceptable and lists measures taken to monitor and protect systems. Consequences of misuse range from the suspension of ICT access to disciplinary action and disclosure to law enforcement agencies.

2.2.2 Awareness raising is covered through policies and procedures, mandatory training, and news items on the corporate intranet.

2.2.3 The mandatory Information Governance training, which covers data protection requirements under the General Data Protection Regulation (GDPR) and Council Information Security requirements (passwords and use of email), is required to be completed by all employees. Completion statistics are reported to the Information Governance Group on a quarterly basis and to each meeting of the Corporate Management Team (CMT), as part of risk Corp-005 Information Governance, included in the Corporate Risk Register. Training completion was 88%, as reported to CMT on 25 July 2019.

2.2.4 There are no OIL courses on risk management, but guidance is available in the Risk Management Framework.

2.2.5 Eleven members of staff were identified as responsible for maintaining information security and for assurance actions in CRR Corp006 and the Cluster risk register for Digital and

Technology. All relevant staff had undertaken the Information Governance training as required.

2.2.6 The Introduction to Information Security page referenced the availability of the For Your Eyes Only information security course; however, the Service has advised there is no longer a requirement to complete this course since the mandatory Information Governance training covers Information Security. The Service has confirmed that the Information Security page has subsequently been updated.

2.3 Risk Registers

2.3.1 The Scottish Government Public Sector Action Plan key action 2 required public bodies to put in place minimum cyber risk governance arrangements by the end of June 2018. As a result, cyber security risks should be included in corporate risk registers and regularly considered by Board-level or senior management staff.

2.3.2 "Cyber Security" has its own listing in the CRR as Corp006 and in the Digital and Technology Cluster Risk Register (DT001). The CRR is owned by the Corporate Management Team (CMT) and is reviewed monthly at CMT. In addition, there is an annual review by the Audit, Risk and Scrutiny Committee. The Cluster Risk Register was last reported to the Operational Delivery Committee on 6 November 2018 and is reviewed by the Cluster management team on a monthly basis. However, there were no records to confirm this monthly review. The Service has confirmed that minutes are now being maintained and separate monthly copies of the Cluster Risk Register will be retained to evidence changes.

2.4 Risk Assessment

2.4.1 All cyber security risks listed in the Corporate and Cluster registers appeared to have been assessed following the guidance provided in the Risk Management Framework. Total baseline risk had been calculated by scoring impact against likelihood; the effectiveness of proposed controls on those scores was predicted; and the residual risk was then calculated.

2.4.2 Corp006 was added to the Corporate Risk Register in 2018, when Corp007 "Information Management and Security" was split into 005 "Information Governance" and 006 "Cyber Security". This links to the Scottish Government's Public Sector Action Plan key action 2, demonstrating the Council's commitment to manage risk from cyber threats. The Service advised that a number of risk causes and controls listed in Corp006 had been added some time ago and there was no paperwork substantiating how they had been identified or giving details of how the risk score had been calculated; however, the risk registers had been compared to those available from similar organisations and from best practice guidance from bodies such as the National Security Cyber Centre (NCSC), and are considered to be comprehensive.

2.4.3 The risk causes and potential impacts listed in Corp006 were reviewed by Internal Audit; they are detailed, relevant and comprehensive, covering causes from human error, through lack of or failure of preventative measures, to lack of recognition of new and existing threats.

2.4.4 The Digital & Technology Cluster Risk DT001 "Service Delivery" is defined as the impact of service disruption on the ability of the Council to deliver key services. A number of the risk causes are related to cyber security, including the use of obsolete domains and operating systems which are no longer supported by the supplier; the use of unauthorised and high risk software; and increased use of the cloud leading to a greater risk of

unauthorised access. The risk causes, as above, are detailed, relevant and comprehensive.

2.5 Risk Controls

2.5.1 The Scottish Government's Cyber Resilience Strategy Public Sector Action Plan Implementation Toolkit describes good practice for organisations when considering risk causes and controls. The guidance also recommends that the National Cyber Security Centre's (NCSC) risk management guidance collection be considered. The risk causes in Corp006 reported to Committee in September 2018 show consideration of the issues raised in Government guidance; they consider lack of oversight and failure to understand threats, human error, network security and insufficient preventative measures, insider and external threats, system vulnerabilities, and maintaining accreditation.

2.5.2 The risk controls listed in the corporate risk Corp006 (as reported to CMT 25 July 2019) were reviewed to confirm they are comprehensive, effective, and follow good practice guidelines.

2.5.3 Controls are listed as fully, partially or not effective. The Service advised that the effectiveness or otherwise of controls was considered on an informal basis within the Service. Those which are not fully effective should link to an assurance action in the next section of the risk entry in the Register. Assurance Actions were listed in CRR Corp006 for every risk control identified as not fully effective as at July 2019.

2.5.4 Versions of the CRR reported between September 2018 and July 2019 were reviewed. Regular updates in the Latest Notes field and in the relevant Assurance Actions section, showed measures being taken to increase effectiveness of controls; all the controls showed either progress or no regression over the reporting period (considered further under section 2.6).

2.5.5 The controls described complied with those recommended in guidance; for example, use of protective monitoring and anomalous behaviour detection tools to control the risk of insider threats and external attacks, and security training and awareness raising of cyber threats for all staff.

2.5.6 The following Cop006 controls were described as "fully effective":

- implementation of protective monitoring (see paragraph 2.1.2 above);
- corporate oversight via Information Governance Board (see paragraph 2.7.6 below);
- effective security training and awareness programme for staff (see section 2.2 above);
- restricted access to key personnel to secure facilities (data centre and cloud provider security reviewed in Internal Audit reports AC1810 and AC1912);
- continual assessment of new and emerging threats (Council's Security Team – covered in AC1810 and AC1912);
- annual IT Health Check (last completed July 2018);
- password security controls in place (covered in AC1912 – ICT Acceptable Use Policy)
- recommended gateway and end point tools in place;
- sufficient staff or resource to investigate events of significance;
- appropriately secured links to all third parties.

2.5.7 Internal Audit has previously reviewed cyber security controls in Internal Audit report AC1810 "Major IT Business Systems" and AC1912 "Data security in a cloud based environment"; and controls were in operation as indicated above.

2.6 Assurance Actions

2.6.1 Risk controls in the registers which are not fully effective should be the subject of Assurance Actions indicating what measures are being undertaken to bring them to full effectiveness, with an owner, a progress rating and a due date. These measures should be updated every time the register is reviewed or reported, particularly if the due date needs to be extended. As stated at paragraph 2.5.3 above, Assurance Actions are listed in CRR006 for every risk control identified as not fully effective.

2.6.2 Since the risks, controls and actions listed in risk DT001 of the D&T Cluster Risk Register link to risk Corp006 of the CRR, assurance actions therein were also reviewed. It was noted that the delivery of an effective staff identity management system (IDAM) was reported as 40% complete in the Cluster risk register but 65% complete in the corporate risk register in July 2019. The Service has agreed to only report progress with the project in the CRR and has since removed the assurance action from the Cluster Risk Register.

2.6.3 Three assurance actions from Corp006 which could be traced from the September 2018 CRR report to the Audit, Risk and Scrutiny Committee through to the version reviewed by CMT in July 2019 were reviewed to confirm that measures undertaken were comprehensive, effective and appropriate. These were: "Develop the use of anomaly reporting"; "Risk assess Critical Business Systems"; and "Develop Cyber Resilience action plan". The original due date had been amended delaying implementation, for the assurance actions "Risk assess Critical Business Systems" and "Develop Cyber Resilience action plan" by fifteen and eleven months respectively. With the exception of the action to risk assess critical business systems, which will require further action once guidance is provided by the Scottish Government, work was progressing to implement the assurance actions towards the revised due dates.

Develop the use of anomaly reporting

2.6.4 Anomaly reporting and behaviour analysis means that a network is constantly monitored for unusual events or trends, such as a spike in internet traffic or bandwidth use; monitoring tools may also react to abnormal behaviour for individual users, for example a log in from a foreign country or multiple failed password entries. It is particularly useful for detecting new threats which may go unrecognised by malware detection tools.

2.6.5 A related action "Investigate methods of, and tools to aid in, identifying and responding to indications of anomalous behaviour", was listed in the CRR reported to the Audit, Risk and Scrutiny Committee on 25 September 2018 "as 50% complete and due to be completed by 30 September 2018, with the update that Identity Access Management and O365 projects were underway as well as a review of Network Management and Monitoring Systems. As reported to CMT, the investigation stage was completed in January 2019, and the investigation action was marked complete, with the January 2019 CMT Assurance Action stating the action will reappear at a later date in order to regularly investigate methods and tools (of identifying and responding to indications of anomalous behaviour).

2.6.6 In the February report to CMT, a related assurance action "Cyber Security 2 – O365/Azure/IDAM" was reported with 60% progress with a due date of 30 September 2019, with the update that as the area developed, security elements needed to be integrated, with the Service providing assurance through the use of a "best practice matrix" detailing required controls. Internal Audit observed that the matrix had been kept updated with progress implementing controls. By the July 2019 report to CMT the action had been renamed to "Develop the use of anomaly reporting" and had progressed to 70%, the due date remained at 30 September 2019, and the notes had been updated to indicate tools provided by Office365 were being explored and developed.

Risk assess Critical Business Systems

2.6.7 This assurance action was first reported to the Audit, Risk and Scrutiny Committee on 25 September 2018 as 80% complete, with the update that a dedicated resource had been allocated to the action, although there was a risk that the due date of 30 September 2018 might not be met. By the version reported to CMT in February 2019 this remained at 80% with an update that systems had been identified but work remained to complete documentation; the date was extended to 30 September 2019.

2.6.8 As at July 2019 this still remained at 80% with the due date postponed to December 2019 in order to document achievement of "baseline" technical and physical measures in accordance with the Scottish Government Cyber Resilience Framework, yet to be made available by the Scottish Government. This work will contribute to the creation of a revised Information Asset Register that reflects all Council systems, describing the nature of the data held and the adequacy of technical and physical controls, as recommended in Internal Audit report AC1912 "Data security in a cloud based environment".

Develop Cyber Resilience action plan

2.6.9 This assurance action is described as necessary to ensure compliance with the Scottish Government's Cyber Resilience Strategy and the measures taken refer to the key actions in the Public Sector Action Plan, such as implementing a "Supply Chain Cyber Security Policy" (key action 8), achieving Cyber Essentials Plus certification (key action 4), and putting in place appropriate cyber incident response plans (key action 7).

2.6.10 The action was first reported in September 2018 as 85% complete, with a due date of 31 October 2018, and an update that preparations were underway for CE Plus assessment and the supply chain policy was under review by ICT and Commercial and Procurement Services (CPS). By February 2019 progress was at 98% with the update that key requirements had been met but some documentation was awaited from the Scottish Government. CPS advised that this had yet to be received from the Scottish Government. CE Plus certification was achieved in July 2018 and as of July 2019 the Service is preparing for re-assessment.

2.6.11 With some key actions complete, the action was amended in April 2019 to refer specifically to the creation of an incident management procedure and progress was reset to 80% with a due date of 30 September 2019. As of July 2019 the amended action was at 90% with the due date remaining at 30 September 2019.

2.6.12 The Service had carried out a low-level Cyber Security Incident exercise, with generally satisfactory results, leading to minor amendments required to enhance the procedure. The Service advised that another, higher-level exercise is scheduled for September 2019.

2.6.13 The Service also advised that guidance and templates covering cyber incident response plans had been received from the Scottish Government as described in the Public Sector Action Plan and a Council Cyber Incident Response Plan has been created based on these. The Plan was reviewed by Internal Audit and was considered to be comprehensive.

2.7 Cyber Resilience

2.7.1 The eleven key actions in the Scottish Government's Public Sector Action Plan were reviewed to confirm that the Council had fulfilled its responsibilities. Work has been undertaken to address the elements of actions which the Council is responsible for, including: governance arrangements (key action 2); participation in the Cyber Security Information Sharing Partnership (key action 3); independent assurance of Council's critical technical controls (key action 4), implementation of cyber security tools; training and

awareness raising (key action 6); and providing written assurance on key actions (key action 11) The remainder are the responsibility of the Scottish Government and the Council cannot act upon them until further information or guidance is received.

2.7.2 The written assurance to the Scottish Government (key action 11) contains details of the Council's work to implement the initial baseline stage of the Scottish Public Sector Action Plan on Cyber Resilience, that is, the measures taken to address the key risks and challenges identified. The responses are provided in a spreadsheet which automatically scores the position from Green+ (completely satisfactory) to Red (completely unsatisfactory). The Council's position was green for all scores with the exception of ACD WebCheck; ACD Protected DNS; Staff Training; and Cyber Incident Response Plan. The score for WebCheck appeared to be an error within the spreadsheet as the response was satisfactory, while the remainder were Amber as they were in the process of being implemented. The Service advised that all have now been fully implemented.

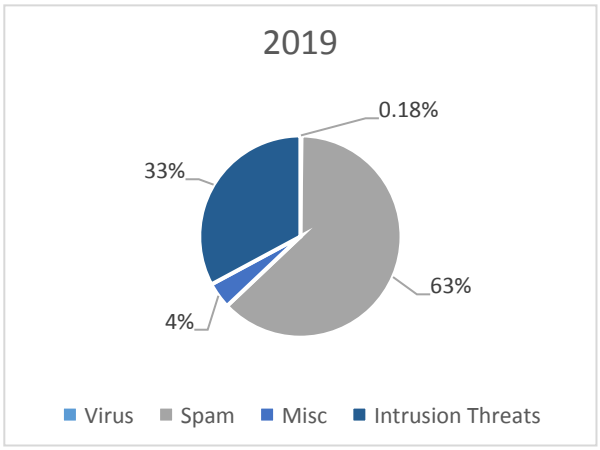
2.7.3 Other standards with which the Council should comply are the Public Sector Network (PSN), provided by central government with the aim of helping public sector organisations work together, reduce duplication and share resources; the government approved IT Health Check (ITHC); and the Payment Card Industry Data Security Standard (PCI DSS), an information security standard for organisations that handle branded credit cards from the major card schemes.

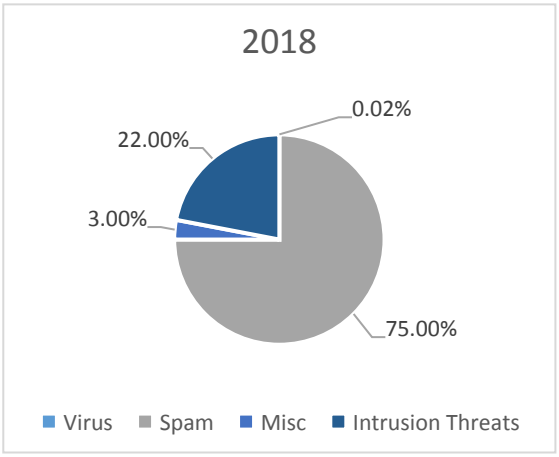
2.7.4 Achieving and retaining PSN accreditation is included in the Digital and Technology Risk Register DT001. The Council is currently not accredited but the update advises this will be re-assessed after the next ITHC. The ITHC has been carried out annually as required; it was last performed in July 2018 and is scheduled to be undertaken again in August 2019. The 2018 assessment found overall levels of security to be good, although a number of passwords were not strong enough and multi-factor authentication was recommended.

2.7.5 The Council is required to comply with PCI DSS in order to take card payments. Requirements include to maintain a firewall to protect cardholder data, protect systems against malware and to track and monitor all access to network resources and cardholder data. The Service provided evidence that the Council was compliant.

2.7.6 Details of attempts to breach the Council's cyber security measures are reported in "Trending Reports" produced by the Information Security team and presented at the Digital & Technology Senior Management Team monthly meetings, and are included in quarterly reports to the Information Governance Group and the Information Governance Management Annual Report which is presented to the Information Governance Group and the Audit, Risk and Scrutiny Committee. Copies of Trending Reports were obtained and had been produced on a monthly basis. They included various statistics, including: cyber risks prevented; email traffic; the Digital and Technology risk register status; and an update on the operational risks of high importance. Copies of the quarterly reports provided to the Information Governance Group were reviewed by Audit and were complete and regular.

2.7.7 Numbers of cyber incident attempts detected and prevented dropped from over 40 million over twelve months in 2018 to 22.5 million over a similar period in 2019. The number and proportion of spam emails fell (approximately 30 million to just over 14 million, 75% to 63%) while there was a lower number but greater proportion overall of intrusion threats, where an attempt is made to compromise system security (approximately 8.9 million to 7.4 million, 22% to 33%). In the twelve months to June 2018 12 attempts were successful and all were successfully mitigated, while to June 2019 10 attempts were successful but all were mitigated.





AUDITORS: D Hughes
A Johnston
L Jarvis

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.