Risk Management Audit Review 2017/18 **Appendix 2**

Introduction

As part of the 2017/18 assurance risk and audit plan, a review has been undertaken of the control activities, policies and procedures currently in place regarding risk management at Allerdale Borough Council (ABC). The aim of this review is to provide management with assurance that the system is robust and operating as intended and provide recommendations for improvement to add value and improve the achievement of objectives.

The objective and scope was defined in the audit brief issued to all relevant staff on 22 February 2018.

Walkthrough testing and results

Area	Control Objective	Control Environment	Assurance Opinion	Commentary
Corporate risks	There are robust arrangements for the identification, evaluation and monitoring of risks and opportunities for achieving strategic objectives	Data integrity; Effective/efficient processes; Effective risk management; Accountability; Value for money	Comprehensive	The Corporate Risks and Issues log is accessed via Share-point. Testing confirmed that the review of the risk log is a regular agenda item on the Senior Management Team meeting and new risks are escalated as they emerge. Managers are encouraged to take ownership of and review their risks regularly adding any new risks as they arise. Responsibilities are assigned and mitigating actions regularly updated. Risks are linked to Council Plan Objectives. Risk management workshops take place every six months, these are well attended by the top two management tiers. Audit Committee risk management training has been provided but this should be encouraged for all members.
Project and Programme risks	There are robust arrangements for the identification, evaluation and monitoring of risks and opportunities for	Effective/efficient processes; Effective risk management; Transparency and accountability; Value for money	Substantial	Testing and discussions with key staff demonstrated that the quality of risk information has improved. The information provided to support key decision making has also improved in this area and there is a demand to improve further. The introduction of the Capital Investment

	achieving project objectives			Strategy and supporting risk analysis, seeks to improve the risk assessment of Capital projects to support decision making and prioritisation based on a number of risk factors. This process is in its infancy and to date only one project has been risk assessed in this way however is considered to be a positive step for the risk management culture at Allerdale. Testing established that the quality of risk information relating to projects identified with the project management software was inconsistent. The quality of risk information and roles and responsibilities for risk management within projects could be improved. This has already been identified as an improvement by the business and the team. Further training is planned for all senior and third tier managers along with a review of the project management documentation.
Operational risks	There are robust arrangements for the identification, evaluation and monitoring of risks to and opportunities for achieving operational objectives.	Effective risk management; Efficient use of resources; Data integrity; Financial viability; Sustainability	Substantial	Testing demonstrated a robust framework in place for all tiers of management to effectively risk manage all aspects of the business. However, there is more work to do to ensure that service risk management is considered following the annual business planning process. The Assurance Risk and Audit Manager is facilitating these discussions with Heads of Service by meeting with them at least annually to discuss risk as part of the annual planning process.

Area for improvement

Number	Recommendation	Associated risks
1	Risk management training should be offered to all members annually.	Risk management, decision making
2	Medium and Low Corporate risks and Service Risks should be reviewed at least 6 monthly as part of the business planning monitoring process.	Risk Management, achievement of objectives

Agreed Action

Number	Agreed Action	Associated risks	Priority	Responsibility, due date and response
1	As part of the programme of improvement to drive a consistent approach to delivering projects by all areas of the business. Training and guidance which clarify roles and responsibilities for project delivery and risk management should be included.	Project Management, Risk management, efficiency and effectiveness and achievement of objectives	Medium	We will improve the project management guidance and information. A project risk workshop will take place in September with support from the ARA team. Consideration of the value of an Assurance Board will be built into the programme management governance going forward. Commissioning Manager 30 Sept 2018.

ICT Audit Review 2017/18

Introduction

As part of the 2017/18 Assurance Risk and Audit Plan, a review has been undertaken of the security controls and procedures in place in respect of the ICT Service at Allerdale Borough Council (ABC). The aim of this review is to provide management with assurance that the security system is robust and operating as intended and provide recommendations for improvement to add value, if appropriate. Areas included: Public Services Network Compliance, security controls, application administration and management of risks and assurances.

Assurance Risk and Audit would like to thank all staff involved during the course of the review for their help and assistance.

The objective and scope for the ICT review was defined in the audit brief issued to all relevant staff on 18 May 2018.

Walkthrough testing and results

	Control Objective	**Control Environment**	**Assurance Opinion**	**Commentary**
Network Security	The organisations networks are protected from attack and unauthorised access and malicious content is filtered out.	Efficient and effective delivery, Compliance, safeguard of assets, data integrity	Substantial internal control Limited PSN Compliance	Allerdale's Network is protected through the use of Evaluation Assurance Level (EAL) 4 certified Firewalls this is an international standard, for the evaluation of an assurance Level that provides a moderate to high level of independently assured security. ICT security measures were tested on 18-19 March 2018 when there was unsuccessful attempts to hack into the council email system. The security measures in place worked successfully and all staff were notified and provided with advice in a timely manner. Testing allowed inappropriate content from an external email into the network and internet security to be easily disabled and therefore unauthorised internet content became accessible **Refer to recommendation 1.**

				Public Services Network (PSN) compliance has not been granted by the Cabinet Office for 2017/18. 2018/19 Public Services Network compliance will not be as onerous as the PSN will only be required for Elections. DWP can use other secure communication networks, ICT have started the implementation of secure emails. The network is independently tested for vulnerabilities on an annual basis as part of the PSN process, the vulnerability report (18.01.2017) showed 235 risks of which 41 were high priority. The number of remedial actions cleared by the ICT team and the detailed action plan to progress these actions had not been provided by ICT at the time of writing this report. **Refer to recommendation 2.**
User education and awareness	User security policies covering acceptable and secure use of systems are in place, staff training provided, and an awareness of cyber risks are maintain.	Efficient and effective delivery, Compliance, safeguard of assets, data integrity, Counter fraud	Substantial	Corporate information management policies are in place however not easily accessible, testing showed that the majority of employees asked struggled to locate the policies. A central store for all corporate policies would be advantageous going forward for the organisation and its policy management. **Refer to recommendation 3.** The quality of user training and awareness on system security and ICT policies is inconsistent throughout the authority. An awareness training session was provided this year however was limited to third tier managers and heads of service. An ICT

				newsletter is produced and circulated to all employees. An information governance E-Learning module is available, however the ability to design and create bespoke modules doesn't exist within the current E-Learning system, there is no function to monitor users agreements to the policies, however compliance to the policies is now written into contracts and users have to agree to accepting these prior to logging onto the network. This process does not provide assurance on users understanding of the policies and their responsibilities. **Refer to recommendation 4.** The organisation has a retention policy which has recently been updated in accordance with GDPR. Office clear out days are organised and additional confidential waste disposal is on hand, however off site facilities still pose a risk in regards to confidential data being stored there. Discussions with the Information and Records Officer presented the opportunity to include corporate scanning information within the retention policy in line with the corporate digital by default approach.
Malware Prevention	Policies and established anti-malware defences in place across the organisation.	Efficient and effective delivery, data integrity	Substantial	The information security policy has information relating to malware, however no specific policy or user guidance exists. The councils ICT estate is protected using a Malware solution (Kaspersky) that has policies applied to all devices to decide what action to take should an issue be found. Given that

				human error is the biggest cause of security breaches the introduction of corporate guidance for users would help mitigate this risk. **Refer to recommendation 5**. Clear screen policy and password requirement is covered in the Information Security Policy, however the length of passwords is not specified, plans are in place to develop single sign on which would mitigate this risk. Different software have different requirements and are not all covered by ICT. **Refer to recommendation 6.**
Removable media controls	Policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.	Efficient and effective delivery, Compliance, safeguard of assets, data integrity, counter fraud	Substantial	Council policy prohibits the use of removable media (USB), it states where such devices have to be used all materials must be encrypted, testing allowed a USB to be used. There is no written procedure which states that ICT must grant access to media options so that they can be scanned for Malware however machines should be blocked from doing this so that the user has to go to ICT, who then would perform the scan. **Refer to recommendation 7.**
Secure configuration	Security patches are applied and the secure configuration of all systems is maintained, a systems inventory exists.	Efficient and effective delivery, data integrity	Substantial	The Council uses Microsoft Intune to manage the estate, all pcs, tablets and phones are registered within the system and policies, patches and software applied. The Solutions Architect (Operations) (SAO) has a monthly patch day, a compliance exercise is completed to ensure all patches are up to date across the estate.

				The organisations systems inventory requires updating to reflect the current position.
Managing user privileges	Establish effective management processes and limit the number of privileged accounts, limit user privileges and monitor user activity, control access to activity and audit logs.	Efficient and effective delivery, Compliance, safeguard of assets, data integrity, counter fraud	Substantial	The three system administrators have enhanced privileges to perform particular actions within a system that standard users do not. Defined roles and responsibilities for system administration are not agreed corporately, therefore these are adopted based on external system training and self-help rather than being based on a level of control agreed by management. This practice creates particular issues when staff leave and new officers are inadequately trained. Getting the most from the systems used should be a key priority as the organisation moves more towards technology based processes. Systems without adequate management reporting functionality or that requires the support of many standalone spreadsheets to support simple processes should be reviewed to confirm they are fit for purpose. **Refer to recommendation 8.**
Performance Management	Appropriate performance indicators are in place to manage the function	Efficient and effective delivery, Compliance, data integrity	Substantial	The organisations KPI data is stored on a shared excel spreadsheet, which is updated and sent to SMT on a monthly basis. Effective processes were in place to monitor statutory and non-statutory deadlines and KPI performance. KPI information is available to all via the shared area and ICT communicate KPI

				information to staff at 1-2-1's and team meetings.

Agreed Actions

Number	Agreed Actions	Associated risks	Priority	Responsibility, due date and response
1	The firewall should be updated regularly to prevent unauthorised content being accessible and external email content filter should be reviewed.	Access to unauthorised sites, potential malicious content allowed into the network, assets and information may be compromised, data breach.	Medium	Solutions Architect (Operations) 23 December 2018
2	The remedial actions detailed on the vulnerability report should be completed with priority given to the critical and high actions that remain outstanding to gain Public Services Network compliance. A detailed action plan should be created and monitored.	Risk being cut off from the network and unable to access critical Whitehall services, for exchanging details of benefits claimants, information may be compromised. Reputational damage, unable to perform services.	High	Completed at the time of the review.
3	Corporate policies should be: • centrally stored • easily accessible • accurate • up to date	Employees and members do not know what is expected from them as a user of Council owned hardware and software, policies are not regularly read as a refresh, user security awareness isn't maximised.	Medium	ICT Manager 30 March 2019
4	ICT Security awareness training sessions should be provided to all employees. An options appraisal should be completed prior to the renewal of the E-learning	Acceptable use and level of information security is not clearly defined Assets and information may	Medium	ICT Manager 23 December 2018

	system contract to establish it has adequate functionality to support learning requirements and is fit for purpose. (HR)	be compromised. Cyber security and information security awareness isn't maximised, data breach.		
5	Due to human error being the biggest cause of security breaches the authority would benefit from corporate guidance for users (posters).	Assets and information may be compromised. Cyber security and information security awareness isn't maximised, data breach.	Medium	Newsletter with interactive features ICT Change Manager 31 October 2018 New Intranet – IT Pages ICT Manager 30 March 2019
6	Procured systems should be configured to Council security levels as part of the implementation. (ER)	Assets and information may be compromised. GDPR breach.	Medium	Completed at the time of the review.
7	The use of media option downloads to allow scanning for malware should be covered in the relevant policy and all machines should be blocked to restrict users from doing so.	Assets and information may be compromised. GDPR breach.	Low	Solutions Architect (Operations) 30 October 2018
8	An organisation standard should be published for application management, to include: Roles and responsibilities for system and technical administration, system security, password and user management, reporting, training and data input and output. To ensure all systems are managed consistently in an effective way and delivering to their maximum potential.	Applications are inconsistently managed Full system functionality is not realised Data quality is compromised Roles and responsibilities are unclear. Cyber security and information management.	Medium	Completed at the time of the review.

Guide to the audit assurance opinions	
Comprehensive	There is a sound system of controls designed to meet objectives, manage risks and controls are consistently applied in all the areas reviewed.
Substantial	There is a good system of controls and risks are managed. However, there are opportunities for improvement in the design or consistency of application that will assist in the achievement of objectives identified as being at risk in the areas reviewed.
Limited	Key controls exist to help achieve objectives and manage principle risks. However, there are opportunities for improvement in the overall control environment which would enhance the design and application of controls, thereby assisting the achievement of objectives identified as being at risk in the areas reviewed.
Minimal	The absence of basic key controls or the inconsistent application of key controls is so severe that the audit area is open to abuse or error. Risks to objectives are not being managed.

Agreed action levels	
High	There is a control vulnerability that could result in failure to achieve corporate objectives, reputational damage, lead to material loss, exposure to serious fraud or failure to meet legal or statutory requirements. This includes material non-compliance with the Constitution, Financial Regulations or Council policies and procedures. Managers should address high priority recommendations urgently to rectify the situation.
Medium	The system or procedure lacks adequate control that could result in failure to achieve operational objectives, non-material loss, or non-compliance with departmental operational or financial procedures. This would also include minor non-compliance with Financial Regulations. Although not fundamental to system integrity these risks should be addressed promptly as the next priority.
Low	To implement this would be good practice to improve or enhance the system and the achievement of objectives. Several low risks in combination may give rise to concern.

In line with the Public Sector Internal Auditing Standards (PSIAS), Assurance, Risk and Audit will monitor all current and future agreed actions. Actions will be recorded in the actions log on Sharepoint including all progress updates whether made by assigned officers directly or by Assurance, Risk and Audit on their behalf. Managers with Network system access have the opportunity to monitor these actions. Implementation dates are agreed before the Final report is issued, amendments to these dates must be agreed with Assurance, Risk and Audit. Agreed actions are monitored by the Senior Management Team and Audit Committee. In the instance that an engagement has not been conducted in line with the PSIAs, the areas of non-conformance will be reported as part of the final report.