

Appendix



RUSHCLIFFE BOROUGH COUNCIL

Internal Audit Progress Report

Governance Scrutiny Group

3 December 2019

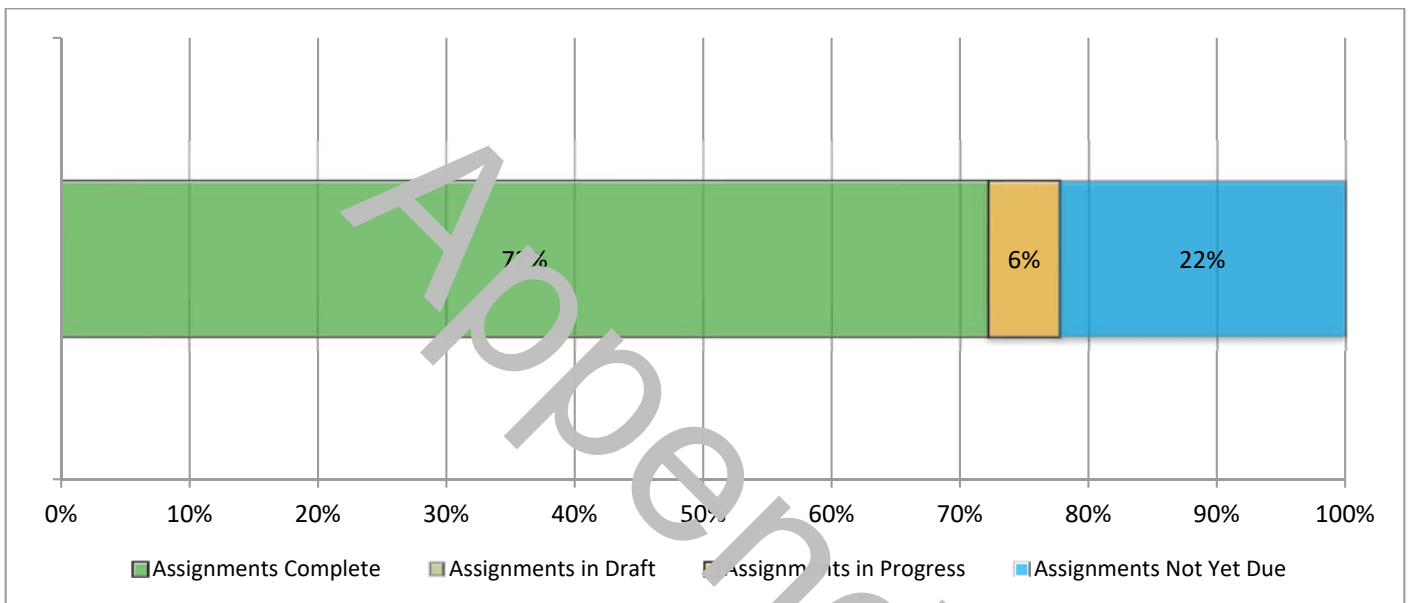
CONTENTS

1	Introduction.....	2
2	Reports considered at this Governance scrutiny group.....	3
3	Looking ahead.....	6
4	Other matters	7
	Appendix A: Internal audit assignments completed to date.....	8
	For further information contact.....	9

Appendix

1 INTRODUCTION

The Internal Audit Plan for 2019/20 was approved by the former Corporate Governance Group on 7 February 2019. Below provides a summary update on progress against that plan and summarises the results of our work to date. Please see chart below for current progress with the Plan.



2 REPORTS CONSIDERED AT THIS GOVERNANCE SCRUTINY GROUP

The Executive Summary and Key Findings of the assignment below is attached to this progress report.

Assignments	Status	Opinion issued	Actions agreed		
			H	M	L
Cyber Risk Management (7.19/20)	Final		0	2	8
Insurance (8.19/20)	Final		0	0	1
Creditors and e-Procurement (9.19/20)	Final		0	0	1
Markets – Review of New Contractual Arrangements (10.19/20)		Advisory	N/A		
Business Support Unit (11.19/20)	Final		0	0	4
Payroll (12.19/20)	Final		0	0	1

2.1 Impact of findings to date



Cyber Risk Management (7.19/20)

Conclusion: Reasonable Assurance

Impact on Annual Opinion: Positive

As a result of testing undertaken, two 'medium' and eight 'low' priority findings were identified. Management actions were agreed in respect of all the findings.

The medium priority findings relate to:

- While a Security Incident Response Plan is in place and incident management roles and responsibilities have been formally defined, the Council does not undertake cyber incident response testing.
 - Although an Intrusion Prevention System (IPS) is in place, our review highlighted that no automated alerts had been configured to notify the ICT Team of a potential incident.
-



Insurance (8.19/20)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing undertaken, one 'low' priority management action was identified, and this was agreed by management.



Creditors and e-Procurement (9.19/20)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing undertaken, one 'low' priority management action was identified, and this was agreed by management.



Markets – Review of New Contractual Arrangements (10.19/20)

Conclusion: Advisory Review

Impact on Annual Opinion: n/a

An advisory review was undertaken to review the actions taken by the Council, when it appointed a new managing agent for the markets operated at Bingham.

Our review confirmed that a new Markets Manager has been selected and a new contract has been put in place to formalise the arrangements between the Council and the Markets Manager. We confirmed that a process of due diligence checks was completed, prior to the contract being signed.

The controls in place, have not been changed significantly following the change in Markets Manager; therefore, if complied with, will continue to be effective in controlling the collection and banking of all income generated from the Council's weekly market in Bingham.



Business Support Unit (11.19/20)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing undertaken, four 'low' priority management actions were identified, and these were agreed by management.



Payroll (12.19/20)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing undertaken, one 'low' priority management action was identified, and this was agreed by management.

Appendix

3 LOOKING AHEAD

Assignment area	Timing per approved IA plan 2019/20	Status
Enforcement – Statutory Nuisance	Quarter 3	Assignment In Progress
Garden Waste	Quarter 3	Not Yet Due
Main Accounting	Quarter 4	Not Yet Due
Property Leases / Rent	Quarter 4	Not Yet Due
Follow Up	Quarter 4	Not Yet Due

Appendix

4 OTHER MATTERS

4.1 Changes to the audit plan

At the request of management an additional advisory audit was undertaken to review the new contractual arrangements for the markets following the appointment of a new managing agent for the markets operated at Bingham.

4.2 Quality Assurance and Continual Improvement

To ensure that RSM remains compliant with the PSIAS framework we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews being used to inform the training needs of our audit teams.

The Quality Assurance Team is made up of: Ross Wood (Manager, Quality Assurance Department) with support from other team members across the Department. All reports are reviewed by James Farmbrough as the Head of the Quality Assurance Department.

This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

4.3 Post Assignment Surveys

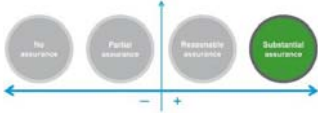





We are committed to delivering an excellent client experience every time we work with you. Your feedback helps us to improve the quality of the service we deliver to you. Currently, following the completion of each product we deliver we attached a brief survey for the client lead to complete.

We would like to give you the opportunity to consider how frequently you receive these feedback requests; and whether the current format works. Options available are:

- After each product (current option);
- Monthly / quarterly / annual feedback request; and
- Executive lead only, or executive lead and key team members.

APPENDIX A: INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

Report previously seen by the Governance Scrutiny Group and included for information purposes only:

Assignment	Status	Opinion issued	Actions agreed		
			H	M	L
Disabled Facilities Grants (1.19/20)	Final		0	1	4
Corporate Governance (2.19/20)	Final		0	0	1
Housing Benefits (3.19/20)	Final		0	0	1
Building Control (4.19/20)	Final		0	3	3
Treasury Management, Cash and Banking (5.19/20)	Final		0	0	0
Land Charges (6.19/20)	Final		0	0	1
Annual Fraud Review	Final	Advisory *			

* A review of the Council's Fraud Annual Report was undertaken and suggestions were provided to management to consider when finalising its Fraud Annual Report.

FOR FURTHER INFORMATION CONTACT

Chris Williams, Head of Internal Audit

chris.williams@rsmuk.com

Address:

RSM Risk Assurance Services LLP
Suite A, 7th Floor
City Gate East
Tollhouse Hill
Nottingham NG1 5FS

Phone: 01159 644450
Mobile: 07753 584993

rsmuk.com

This report is solely for the use of the persons to whom it is addressed. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Rushcliffe Borough Council, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

CYBER RISK MANAGEMENT - DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/ reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Risk: Loss of information, risks from inappropriate and malicious access, viruses and malware and of legal action/ loss of reputation due to inappropriate storage of/ sharing of personal data.								
1	Secure Configuration Vulnerability scans are performed on a regular basis. Vulnerabilities identified on a quarterly basis using Nessus scans are classified and a timeframe for rectification is agreed.	Yes	No	We confirmed through observation that scans are performed against all network devices on a quarterly basis using Nessus. Vulnerabilities identified during these scans are recorded within a 'Nessus Remediation Plan' for that quarter. Details within this Remediation Plan include: <ul style="list-style-type: none"> • Probability; • Risk; • CVSS Score, (Common Vulnerability Scoring System); • Recommended fix; • Owner; 	Low	Management will ensure that the vulnerability remediation tracker is completed to include assigned remediation owners and expected completion dates.	30 November 2019	ICT Service Support Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<ul style="list-style-type: none"> • Status; and • Target and actual completion dates. <p>However, review of the NESSUS Remediation Plan Q2 2019-20, highlighted gaps within the completion of the Plan at the time of our review. We noted high and medium probability vulnerabilities that did not have assigned owners, target completion dates, or clearly documented status. We were informed by the ICT Manager that assigned remediation, owners and expected completion dates are followed; however, on this occasion the team had failed to populate the spreadsheet with the required fields.</p> <p>If vulnerabilities that have been identified are not assigned responsibility and an agreed timeframe outlined there is a risk that, due to lack of accountability, vulnerabilities are not remediated, thus increasing the risk of a cyber incident.</p>				
2	Network Security and Firewalls The firewall rule base is reviewed on a periodic basis and the rules are accompanied with a description.	Yes	No	We observed a test change being made to the firewall rule base, which confirmed that an audit trail is retained with the name of the user that made the change alongside the date and time. However, further inquiry with the ICT Technical Solutions Officer highlighted automated notifications	Low	Management will review the firewall settings and confirm if it is possible to set up an automated notification system to send email alerts when a change is made to the firewall rules.	31 October 2019	ICT Technical solutions Officer

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	The Council has a documented Change Management Policy for administering changes to the firewall.			<p>were not configured to alert IT staff automatically if any changes were made to the firewall settings; such as, if rules were added, removed or disabled.</p> <p>Automated alerts notifying the IT Department of changes to a firewall rule base can be useful as an early indicator or warning mechanism of a cyber security incident. There is a risk that changes may be spotted too late or missed if reliant on a manual reconciliation, potentially leading to a cyber incident.</p>				
3	<p>User Education and Awareness</p> <p>Staff are trained on Cybercrime; phishing, smishing and vishing' upon their induction and on an annual basis.</p>	Yes	No	<p>We obtained and reviewed the course completion status for all staff which confirmed for 216 staff enrolled, only nine had not completed the course putting the compliance rate at the time of our review at 96%.</p> <p>A completion rate of less than 100% poses a risk of some staff not being fully aware of cyber risks and the actions that they can take to prevent them, this raises the likelihood of a cyber incident.</p> <p>We were informed by management that the compliance rates for e-learning modules is monitored by HR and that reminder emails are sent to ensure completion. Further review of the course completion status highlighted that all the users identified that had not completed the 'Cybercrime; phishing, smishing and</p>	Low	<p>Management will ensure that the compliance rate for the cyber security training is 100%, any exceptions will be followed up to ensure that training is completed. Appropriate action will be considered for users that do not complete the training after escalation.</p>	31 December 2019	All Lead Specialists

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>ishing' course had been enrolled onto the course for at least 6 months. We noted from discussion with the ICT Manager that this was an issue that they were aware of and despite escalation to Line Managers, some users were still not completing the training as required.</p> <p>If non-compliance not appropriately escalated and remediated, there is a risk that some staff will not complete the training and therefore will not be fully aware of cyber risks and the actions that they can take to prevent them, this raises the likelihood of a cyber incident.</p>				
4	<p>User Education and Awareness</p> <p>The Council have not yet conducted any phishing exercises.</p>	No	-	<p>We were informed by the ICT Manager that the Council has not yet undertaken any phishing exercises with a view to determine the vulnerability level of its network, which would provide an indication of how many people may be susceptible to an email-borne social engineering attack.</p> <p>Therefore, there is a risk that staff will not be fully conscious of cyber and data security threats and issues. This may result in staff being more susceptible to a cyber-attack, which may pose a vulnerability to the Council.</p> <p>This is mitigated in part by the fact that phishing is included within the e-learning that is provided to staff. We were also informed by the ICT</p>	Low	Management will ensure that annual phishing exercises are undertaken to test user awareness and to ensure that they remain conscious of cyber security issues.	31 March 2020	ICT Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				Manager that ICT Services are looking to implement phishing exercises using tools within Office 365.				
5	<p>Incident Management</p> <p>A Security Incident Response Plan is in place. Incident management roles and responsibilities have been formally defined.</p> <p>The Council does not undertake cyber incident response testing.</p>	No	-	<p>Review of the Cyber Incident Response Plan confirmed that an incident response team was outlined with associated responsibilities of each team member.</p> <p>We were informed by the ICT Manager that no cyber security related incidents had occurred in the past 12 months.</p> <p>While the Incident Management Plans cover a range of security incidents that could occur including the high risks acknowledging that not every scenario possible can be documented. The ICT Manager has stated that the plans will continue to be enhanced to develop additional scenarios in line with developing threats.</p> <p>Discussion with the ICT Manager highlighted that although the Council conduct Disaster Recovery testing for the IT Environment, historically they have not undertaken any testing of their cyber incident management process. However, this is being reviewed and scheduled to take place this financial year. Testing provides added assurance that response plans are effective in reporting and managing a cyber incident. Additionally, testing helps to increase</p>	Medium	<p>Management will ensure that the Cyber Incident Response Plan is tested annually, and the lessons learned will be captured and feed back into the process.</p> <p>Management will ensure that work underway to expand potential cyber incidents is completed, this will help to assist in planning scenario testing.</p>	31 March 2020	ICT Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>awareness of staff and can identify opportunities for improvement.</p> <p>As a result, there is an increased risk that the Council is not fully equipped to deal with information security or cyber incidents effectively, causing increased disruption and greater impact of incidents. It also presents a missed opportunity for learning developments around incident responses and potential for improvement.</p>				
6	<p>Managing User Privileges</p> <p>Domain administrator privileges have been provided to a restricted selection of IT staff.</p>	Yes	No	<p>We reviewed each domain administrator account on the Council's network to confirm that access was required and appropriate. Annual reviews of privileged access are currently performed; however, more frequent reviews will ensure that any inappropriate access is identified and then removed earlier.</p> <p>Increasing the frequency of the periodic reviews of privileged access such as members of staff or third parties that have administrative accounts; can reduce the risk that a user might be able to access information which may no longer be relevant for their job roles, which could lead to abuse of privileged access and compromise of the Council's data and systems.</p> <p>We note that Only ICT staff have the ability of creating Domain</p>	Low	<p>Management will ensure that there is a review of privileged user accounts on at least a bi-annual basis. Particular attention will be paid to domain administrator accounts.</p>	31 December 2019	ICT Service Support Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				Administrator accounts and are the only users with these privileges.				
7	<p>Managing User Privileges</p> <p>There is no monitoring in place around domain administrator accounts</p>	No	-	<p>Discussion with the ICT Technical Solutions Officer highlighted that there is no monitoring solution in place for domain administrator accounts.</p> <p>Without a monitoring solution in place for domain administrator activity, such as password changes, account lock out, and creation of another admin accounts, there is a risk that early indicators of cyber incidents are missed.</p>	Low	<p>Management will consider implementing monitoring activities around domain administrators e.g. promotion to admin, changed passwords, etc.</p>	31 December 2019	ICT Technical solutions Officer
8	<p>Removable Media</p> <p>The use of removable media is limited. Authorisation is required to access removable media devices.</p> <p>Review processes are not in place to control or manage the ongoing use of removable media.</p> <p>Removable media drive access is only permitted with encryption. This is enforced at a group policy level.</p> <p>Users are permitted to use their own</p>	No	-	<p>By default, users read and write access to removable media devices is blocked. We confirmed that a network group is in place that allows select users to read and write to an encrypted removable media device.</p> <p>Review of the Removable Media Policy confirmed that, when authorised by the relevant Executive Manager, Service Manager or Lead Specialist, removable media used should be encrypted.</p> <p>For a sample of 5 users with access permissions for removable media, we located the documented approvals for 4 of the users.</p> <p>We tested a sample of ten user devices throughout the Council's office by using an unencrypted USB storage device and confirmed that removable media was blocked on six users'</p>	Low	<p>Management will ensure that the use of user owned, encrypted, removable media devices on the Council's IT environment is reviewed and management are happy with the risks associated with this practice.</p> <p>If management decide to restrict removable media devices to Council owned devices:</p> <p>Management will ensure that as part of the user access review that users with removable media permissions are reviewed and confirmed that that the permission is still necessary.</p>	31 December 2019	ICT Service Support Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	removable media device, if encrypted.			<p>devices. The user devices that allowed removable media access would only allow access once the USB storage device was encrypted. We confirmed that the four users were part of the network group that allowed encrypted removable media use.</p> <p>We were informed that there is no review of the network group that allows write access to encrypted removable media.</p> <p>If users with access permissions to removable media are not reviewed there is a risk that permissions are given to users that no longer require them. The greater the number of access to removable media the greater the risk is of data loss and a potential cyber incident.</p> <p>We noted that users are able to use their own USB removable media devices if encrypted. This poses a risk that data that is stored on these devices is not returned once that user leaves the Council. Additionally, the Council are unable to keep track of personal removable media devices and therefore could be unaware of potential data loss.</p> <p>Further inquiry with the ICT Technical Solutions Officer highlighted that an asset register is not kept of the location of removable media devices that are permanently given to staff.</p>		<p>Management will ensure that a clear audit trails for USB permissions is retained, this will be part of the review process.</p> <p>Management will ensure that removable media devices that are given out on a permanent basis are recorded on the asset register to recover upon that users leaving date.</p>		

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				This increases the risk that the asset could be lost or not returned without the Council's knowledge, potentially leading to unauthorised access to data.				
9	<p>Monitoring</p> <p>The Council has tools in place for monitoring activity on the network.</p> <p>The Council's Check Point firewall employs Intrusion Prevention System (IPS) on the network to identify and prevent any network security vulnerabilities and monitor traffic for unusual activity.</p>	No		<p>The Council has a number of monitoring tools in place such as:</p> <ul style="list-style-type: none"> • Antivirus software has monitoring capabilities; • Firewall and IPS maintain logs of network activity; • Web and email filtering activity logs; and • Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer that is connected to the network. <p>However, in discussion with the IT Manager we were informed that there is no coordinated, proactive review of all security logs to identify security events in a timely manner; therefore, the Council will be unable to minimise the damage that is done to the network or prevent a data breach.</p> <p>We confirmed through observation that the Council's firewall solution, Check Point, logs network authentication activity, including failures, and is captured and retained for six months. Inquiry to the ICT</p>	Medium	<p>Management will consider the costs and benefits of implementing a SIEM solution to collate all security log information and report potential incidents through automated alerts. These alerts will be reviewed regularly to identify security threats to the network.</p> <p>Management will ensure that informative data, extracted from firewall logs is reviewed on a regular basis.</p> <p>Management will ensure that the IPS in place is configured to send automated alerts notifying the IT Team of a potential cyber incident.</p>	31 March 2020	ICT Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>Technical Solutions Officer highlighted that the firewall log was not reviewed on a regular basis. We were further informed by the ICT Manager that the data captured from the firewall logs and IPS doesn't provide the Council with anything informative without a lot of investigative work and that he is currently looking to introduce a SIEM product to provide informative data.</p> <p>If firewall logs are not reviewed on a regular basis, there is an increased risk that early indicators to cyber incidents are missed.</p> <p>Further observation of the Check Point configuration confirmed that an IPS was enabled. However, a query highlighted that no automated alerts had been set up.</p> <p>We have noted from the ICT Manager that the IT department will be reviewing the IPS rules annually and notifications to enhance security levels and implement automated alerts. Without automated alerts from the IPS there is an increased risk that a cyber incident could occur without detection, increasing the impact of the cyber event down the line.</p> <p>A security information and event management (SIEM) tool can be used to pull together all of the monitoring logs which can enable IT to review exceptions identified via one tool rather than multiple tools.</p>				

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>Whilst the monitoring tools in place can improve the security and effectiveness of the IT Department a SIEM tool can reduce the risk of an alert being missed due to the number of tools in place. SIEM is a step forward to strengthen existing set of network security controls.</p> <p>In the absence of proactive monitoring, there is an increased risk that a security breach will go unnoticed leading to business disruption and data loss resulting in financial loss and regulatory fines.</p>				
10	<p>Monitoring</p> <p>On a quarterly basis the IT Team produces Management Information (MI) packs on IT performance and these are reported to the Senior Management.</p>	Yes	No	<p>We were informed by the ICT Manager that MI packs are currently put together for senior management on a quarterly basis; however, details regarding cyber security are limited to reporting compliance with standards, such as PCI DSS.</p> <p>This in turn could result in a lack of priority and resourcing for the cyber security matters to ensure ongoing identification and mitigation of threats and safeguarding of the Council's information assets and systems.</p>	Low	<p>Management will ensure that MI packs include information regarding all cyber related exceptions and outstanding and remediated vulnerabilities.</p> <p>The packs may include but are not limited to the following:</p> <ul style="list-style-type: none"> • Incidents raised and resolved • Patching status • Antivirus status • Changes to the IT environment • Uptime and availability • Vulnerability scan results and actions. 	31 January 2020	ICT Manager