INTERNAL AUDIT PROGRESS REPORT

Brentwood Borough Council

2022/23

IDEAS | PEOPLE | TRUST

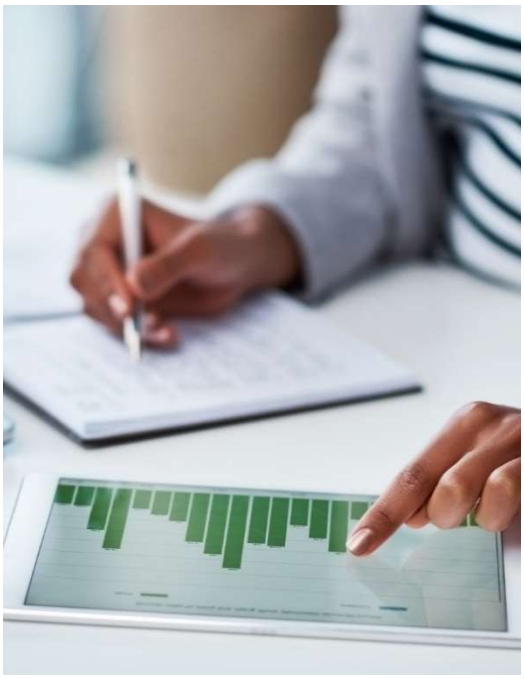
BDO

CONTENTS

SUMMARY OF 2022/23 WORK

INTERNAL AUDIT

This report is intended to inform the Audit and Scrutiny Committee of progress made against the 2022/23 internal audit plan. It summarises the work we have done, together with our assessment of the systems reviewed and the recommendations we have raised. Our work complies with Public Sector Internal Audit Standards. As part of our audit approach, we have agreed terms of reference for each piece of work with the risk owner, identifying the headline and sub-risks, which have been covered as part of the assignment. This approach is designed to enable us to give assurance on the risk management and internal control processes in place to mitigate the risks identified.



INTERNAL AUDIT METHODOLOGY

Our methodology is based on four assurance levels in respect of our overall conclusion as to the design and operational effectiveness of controls within the system reviewed. The assurance levels are set out in Appendix 1 of this report and are based on us giving either 'substantial', 'moderate', 'limited' or 'no'. The four assurance levels are designed to ensure that the opinion given does not gravitate to a 'satisfactory' or middle band grading. Under any system we are required to make a judgement when making our overall assessment.

2022/23 INTERNAL AUDIT PLAN

Our reporting on individual audits is later than would normally be the case, primarily due to a delayed start in the audit programme for the year (which could not be started until we were contractually engaged and the audit plan was approved) and further delays experienced in securing audit start dates and receiving requested information.

However, we are making progress in delivering the audit programme and we are pleased to present the following report to this Audit and Scrutiny Committee meeting:

- Cyber security

The following audits are at completion stage:

- Partnership with Rochford
- Environment - fly tipping, street cleaning and enforcement
- Climate change advisory review
- Licensing
- Sheltered accommodation

Fieldwork is in progress on the following audits:

- Main financial systems and Financial systems advisory review
- Leisure services

The Commercialisation, Payroll and Policy review audits are being planned and are expected to be completed over the next couple of months.

CHANGES TO THE 2022/23 INTERNAL AUDIT PLAN

At officers' request, we have changed the Housing Information audit into an audit of Sheltered Accommodation. We have also agreed to carry out a financial systems advisory review alongside our audit of the main financial systems, and to carry out the Climate Change review on an advisory basis.

REVIEW OF 2022/23 WORK

AUDIT	COUNCIL LEAD	AUDIT COMMITTEE	PLANNING	FIELD WORK	REPORTING	DESIGN	EFFECTIVENESS
Main financial systems and Financial systems advisory review	Interim Director Resources	June/July 2023	✓	✓			
Commercialisation and cost savings	Interim Director Resources	June/July 2023	✓				
Payroll shared service	Interim Director Resources	June/July 2023	✓				
Partnership with Rochford	Strategic Director	June/July 2023	✓	✓			
Policy review	Director Policy and Delivery	June/July 2023	✓				
Data protection	Interim Director People and Governance	June/July 2023	✓				
Cyber security	Corporate Manager IT & Service Improvement	March 2023	✓	✓	✓	M	M
Sheltered accommodation	Corporate Manager - Housing Needs and Delivery	June/July 2023	✓	✓			
Environment - fly tipping, street cleaning and enforcement	Director Environment and Director Communities and Health	June/July 2023	✓	✓			
Climate change	Director Environment	June/July 2023	✓	✓			
Leisure services	Corporate Manager Communities, Leisure and Health	June/July 2023	✓	✓			
Licensing	Environmental Health and Licensing Manager	June/July 2023	✓	✓			
Democratic services	Corporate Manager (Democratic Services)	January 2023	✓	✓	✓	M	M

CYBER SECURITY AUDIT

CRR REFERENCE: RSK 13: CYBER THREATS

Design Opinion	M Moderate	Design Effectiveness	M Moderate
Recommendations	1	1	2

SCOPE

BACKGROUND

- Information Technology (IT) systems enable the Council to provide its critical services to its residents and customers and are used to collect, process and retain ever increasing amounts of confidential information. The vulnerabilities that exist in these IT systems, as well as the infrastructure that supports them, combined with a perceived lack of awareness regarding security issues, have led to attackers targeting public sector organisations and expose the Council to the risk of a cyber security attack.
- Cyber security is the practice of defending the Council's IT infrastructure, networks, and data from malicious attacks, including computers, servers, mobile devices and electronic systems. Cyber security attacks can be launched from any internet connection and, as recent examples across the public sector have demonstrated, they can have a significant financial and reputational impact on the Council and can affect its ability to operate and provide its critical services to the public.
- The UK Government published a Cyber Security Breaches Survey 2022 report, which provides a detailed overview comprising both quantitative and qualitative research and details the cost and impact of cyber breaches and attacks on UK businesses, charities, and educational institutions. The survey found that 39% of organisations had identified a cyber-attack over the past 12 months. The most common attack vector remained phishing mails (83%), but one-in-five of these organisations identified a more sophisticated attack such as a denial of service, malware, or ransomware.
- We completed a cyber security audit in March 2021, which assessed the Council's cyber security controls and concluded moderate assurance over both their design and their operational effectiveness. The key findings arising from the review included the absence of cyber security awareness training, the absence of a defined, finalised and approved cyber incident response plan and the lack of internal vulnerability scans on the Council's IT network.
- We completed a separate audit review of IT/Data Breaches in September 2021, which also highlighted the lack of training in place to increase cyber security awareness amongst members of staff. This review provided substantial assurance over the Council's controls for responding to IT and data security breaches and moderate assurance over their operational effectiveness.

AREAS REVIEWED

- We have reviewed cyber risk assessments, network diagrams, information security policies and procedures, operating systems and application updates, firewall rules, access to the network management console, antivirus updates, domain administrator access rights, external penetration tests and internal vulnerability scans, incident response plans, data recovery and restore plans, and cyber awareness training.

AREAS OF STRENGTH

We identified the following good practice:

- Agendas and papers for meetings are uploaded onto the Council's website for Ordinary Council, Extraordinary Council and Committees at least five days before the meeting, as required by the Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012
- The Council's Strategic Risk Register and Operational Risk Register both contain entries relating to risks around cyber security, with each entry recording appropriate owners, risk scores, mitigating actions and further actions to take. The mitigating actions for each cyber security risk entry rely upon the work of Hytec, the Council's managed security operations centre (SOC) service provider. Updates to the risk registers are reported to the Audit and Scrutiny Committee on a quarterly basis.
- The SOC provides robust defence mechanisms to prevent and mitigate the risk of cyber security attacks. These are underpinned by an OODA ('observe, orient, decide, act') loop process chart to demonstrate how threats are identified and dealt with on a daily basis. The SOC also has a Council-specific knowledgebase to draw upon in managing and addressing threats which, in turn, are managed using AlienVault. The Council also utilises alliances with other organisations through Essex Online Partnership (EOLP) to share threat intelligence, knowledge and resources in relation to cyber security.
- Key components of the Council's IT infrastructure are set out in network topology diagrams, including Microsoft Azure DMZ, Azure Network Security Groups, Internet Facing Servers and Production RDS Environment. The network topology confirmed there to be clear segregation between trusted and untrusted networks, with external traffic passing through virtual networks and firewalls for example. In addition, our testing confirmed that specific firewall rules and DMZ configurations are set for individual business applications, which are hosted on their own virtual machines.
- Domain Administrator accounts are assigned within Active Directory in accordance with the principle of least privilege. There are 18 Domain Administrator accounts in total, which are split between system generated accounts and individual user accounts. Each of the Domain Administrator user accounts we tested was found to have been assigned varying levels of user group access instead of all accounts having the same default level of access. Furthermore, each Domain Administrator is also assigned a regular user account for conducting day-to-day activities, resulting in privileged accounts being used only for administrator tasks.
- Updates to the Council's Windows systems are managed using Microsoft Endpoint Manager (MEM). Automatic updates have been enabled for the Windows OS, Microsoft products (e.g. Office 365) and system drivers, in line with Microsoft's 'Patch Tuesday'. Devices therefore receive updates as soon as they are released and the option to pause Windows Updates has also been disabled. Furthermore, all devices are set to automatically enable the use of anti-virus, anti-spyware and anti-malware software, whilst also requiring the device to comply with a machine risk score of 'Low'.

AREAS OF CONCERN

Our work highlighted the following areas of concern:

- While the Council has a suite of policies in place pertaining to information governance and security, our review of ten policies found them to be out of date, with their last review dates being between February 2009 and March 2018. Additionally, we noted that there were several gaps within the policies, including lack of reference to relevant legislation such as UK GDPR and redundant references to other policies and documentation. Additionally, the Information Security Policy, which is dated July 2017, is still in draft format and has not been approved and finalised (Medium – Finding 1).

- Hytec uses the Nessus Vulnerability Assessment tool to scan external IPs/interfaces for the Council, serving as a form of quarterly external penetration test rather than the traditional method of carrying out external penetration testing on an annual basis. The output report in November 2022 showed there to be 40 vulnerabilities, five of which remained from the scanning undertaken in September 2022. In addition, Hytec performs internal vulnerability scans using the tool on a weekly basis and the figures from 12 December 2022 showed a total of 3,744 vulnerabilities, 1,283 of which were assigned a 'High' priority. Management informed us that the vulnerabilities are prioritised, remediated and monitored using knowledge and expertise of staff, however there are no formal action plans in place to capture this work or to escalate risks and issues to senior management on a regular basis (High – Finding 2).
- The Council has mandatory e-learning in place for staff titled 'Information Governance Level 2'. The e-learning covers topics which are critical to the way that the Council processes and stores information, including sections on data security, the Data Protection Act 2018 and data handling/storage. A report of all staff who have carried out the Cyber Awareness training showed that of the 300 individuals who have completed the training, ten had not achieved the required pass score of 80% (Low – Finding 3).
- Although the Council has a Cyber Incident Response Plan in place, which is reviewed on an annual basis and last updated in June 2022, there is no reference made within the Plan to Hytec's operations as the Council's SOC service provider. Our discussions with management and Hytec identified that a proactive monitoring, escalation and investigation process takes place for potential cyber security incidents, rather than following a specific, documented process for individual scenarios. However, this process, Hytec's role and communication between the two parties has not been documented in the Plan (Low – Finding 4).

CONCLUSION

- The Council has effective processes in place for the monitoring of its infrastructure in addition to responding to cyber incidents and threats by working proactively with its managed service provider, Hytec. However, potential risks and vulnerabilities should be identified, escalated and addressed in a timely manner. Improvements are also required to ensure that policies and processes are robust, accurately documented and communicated to staff.
- We have raised one high priority, one medium priority and two low priority recommendations to improve the Council's cyber security controls and procedures.
- Consequently, we conclude moderate assurance over the design of the Council's cyber security controls as well as their operational effectiveness.

MANAGEMENT ACTION PLAN:

Recommendation	Priority	Management Response	Responsible Officer and Implementation Date
Outdated policy documentation The Council's suite of IT policies and procedures should be reviewed on an annual basis in accordance with a defined review schedule. The Council should also consider amalgamating policies where appropriate, or reviewing and updating the policies on a staggered basis due to the number of policies owned by the Council, reducing the administrative burden on staff.	Medium	Agreed – the suite of IT policies and procedures will be reviewed and updated where necessary. We will also add to the procedures annual review of these which aligns with the adoption of the Continuous Service Improvement model.	Corporate Manager for IT and Service Improvement 30 September 2023
Remediation of vulnerabilities The Council should ensure that vulnerabilities identified in the external Nessus scans and internal vulnerability scans are summarised and reported to senior management on a regular basis for the purposes of: • Informing senior management of the potential risks posed to the Council's IT infrastructure and underlying information assets • Prioritising and remediating vulnerabilities on a timely basis, in line with the Council's risk appetite and target risk scores specified in risk registers • Ensuring that sufficient resource is allocated to managing and remediating vulnerabilities.	High	Agreed – we will update our processes from using the most recent report to inform work to adding in a review and remediation prioritisation of vulnerabilities. We will develop a risk/security dashboard to provide relevant information to the Director of Data and Customer Insight.	Corporate Manager for IT and Service Improvement 30 June 2023
Information governance training Where staff achieve less than the threshold of 80% for the Information Governance training, they should be prompted to complete the training again.	Low	The Council has adopted and as of February gone live with a new eLearning platform providing relevant eLearning courses for GDPR and Cyber Awareness. IT will work with HR and ELT managers for compliance and the demonstration of the appropriate level of knowledge. This is now Business as Usual and will be focusing on the GDPR courses first.	Corporate Manager for IT and Service Improvement 30 April 2023

Recommendation	Priority	Management Response	Responsible Officer and Implementation Date
Cyber incident response plan The Council should amend and update its Cyber Incident Response Plan to include the role of Hytec, specifically how AlienVault is used to monitor cyber security events and the process for escalating threats to the Council for further investigation.	Low	The Cyber Incident Response Plan will be updated to address the above recommendation.	Corporate Manager for IT and Service Improvement 31 May 2023

KEY PERFORMANCE INDICATORS

QUALITY ASSURANCE	KPI	RAG RATING
1. Annual Audit Plan delivered in line with timetable.	A number of audits have been deferred, as detailed on page 3.	A
2. Actual days are in accordance with Annual Audit Plan.	We are on track to meet this KPI.	G
3. Customer satisfaction reports – overall score at least 70% for surveys issued at the end of each audit.	No survey responses received yet for 2022/23.	N/A
4. Annual survey to Audit Committee to achieve score of at least 70%.	Annual survey for 2022/23 not yet completed.	N/A
5. At least 60% input from qualified staff.	This KPI has been met in audits completed to date.	G
6. Issue of draft report within 3 weeks of fieldwork 'closing' meeting.	This KPI has been met for 2 out of 2 audits (see table below).	G
7. Finalise internal audit report 1 week after management responses to report are received.	This KPI has been met for 2 out of 2 audit (see table below).	G
8. Positive result from any external review.	Following an External Quality Assessment by the Institute of Internal Auditors in May 2021, BDO were found to 'generally conform' (the highest rating) to the International Professional Practice Framework and Public Sector Internal Audit Standards	G
9. Audit sponsor to respond to terms of reference within one week of receipt and to draft reports within two weeks of receipt.	The KPI regarding Council agreement of the terms of reference has been met for 5 out of 11 audits (see table below). The KPI regarding draft report has been met for 2 out of 2 audits (see table below).	A
10. Audit sponsor to implement audit recommendations within the agreed timeframe.	Of the recommendations raised to date for 2022/23, the one recommendation due has been implemented.	G
11. Internal audit to confirm to each meeting of the Audit and Scrutiny Committee whether appropriate co-operation has been provided by management and staff.	We have experienced some delays in securing meetings to start our audits and in receipt of information to complete our audits.	A

AUDIT TIMETABLE DETAILS (2022/23AUDITS)

Audit	Draft TOR issued	Management response to TOR received	Closing meeting	Draft report issued	Management response to draft report received	Final report issued
Main financial systems	24/01/23	24/01/23 (KPI 9 met)				
Financial systems advisory review	25/01/23	26/01/23 (KPI 9 met)				
Commercial-isation and cost savings						
Payroll shared service						
Partnership with Rochford	23/12/22	12/01/23 (KPI 9 not met)				
Policy review	15/02/23	Not yet received (KPI 9 not met)				
Data protection						
Cyber security	16/09/22	29/09/22 (KPI 9 not met)	20/01/23	06/02/23 (KPI 6 met)	16/02/23 (KPI 9 met)	23/02/23 (KPI 7 met)
Sheltered accommod-ation	02/12/22	05/12/22 (KPI 9 met)				
Environment - fly tipping, street cleaning and enforcement	02/12/22	15/12/22 (KPI 9 not met)				
Climate change	25/01/23	02/02/23 (KPI 9 not met)				
Leisure services	13/02/23	13/02/23 (KPI 9 met)				
Licensing	28/11/22	01/12/22 (KPI 9 met)				
Democratic Services	10/03/22	08/04/22 (KPI 9 not met)	11/01/23	11/01/23 (KPI 6 met)	11/01/23 (KPI 9 met)	13/01/23 (KPI 7 met)

KEY FOR RAG RATING:

G = met target

A = partly met target

R = not met target

= not applicable

APPENDIX 1

OPINION SIGNIFICANCE DEFINITION

LEVEL OF ASSURANCE	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION	FINDINGS FROM REVIEW
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main, there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE DEFINITION

RECOMMENDATION SIGNIFICANCE	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

FOR MORE INFORMATION:

GREG RUBINS

Greg.Rubins@bdo.co.uk

JANINE COMBRINCK

Janine.Combrinck@bdo.co.uk

www.bdo.co.uk