

30th JANUARY 2023

INTERNAL AUDIT – AUDIT UPDATE

SUMMARY:

This report describes:

- The work completed by Internal Audit since the last report;
- A progress update on the 2022/23 Audit Plan; and
- An update on outstanding audit issues.

RECOMMENDATION:

Members are requested to:

- i. Note the audit work completed since the last update.
- ii. Note the update to the deliverables for Quarters 4.
- iii. Note the outstanding audit issues.

1 Introduction

1.1 This report is to provide Members with:

- An overview of the work completed since the update provided to the Committee in November 2022;
- A progress update on the 2022/23 Audit Plan;
- A schedule of work to be delivered in Q4; and
- An update on the outstanding audit issues, highlighting any significant risk exposures or control issues.

2 Audit Work Completed

2.1 The table below provides an overview of the assurance opinion, given to the completed audit since the last update:

Audit Title	Assurance Opinion	Recommendations by Priority		
		High	Medium	Low
2022/23 Internal Audit Plan				
Financial Grants to Organisations	Substantial	0	0	0
Cyber Security	Reasonable	3	16	4

2.2 Below is a summary of the key findings from the audits.

Financial grants to organisations

The four grant schemes that local organisations can apply for are well managed and soundly run. There are defined processes that include a robust assessment of applications, independent review and approval, and verification that the funds are being used for the intended purpose.

There are four value-added observations which have been provided to enhance the current good processes in operation.

Cyber Security

The Council has a comprehensive, multiyear Cyber Plan, setting out a range of interlinked initiatives to enhance its cyber defences over the medium term, based on National Cyber Security Centre (NCSC) guidance. However, the Plan needs to be finalised (as planned).

The most recent assessments to support Public Services Network (PSN) assurance are positive regarding the strength of firewalls, user management infrastructure (Active Directory) and the Virtual Private Network (VPN), However, there were vulnerabilities and outstanding actions, which pose risks to the Council until addressed and these need to be better captured/documented.

The Council's Patching Policy needs to be finalised with zero-day and cyber response processes/ plans documented and tested.

For systems that are managed outside of IT, good practice is for there to be a clear segregation of duties (SoD) for key technical processes: requesting, authorising and granting access to systems. Arrangements for a sample of systems were reviewed, with very limited SoD observed. This represents a clear risk with potential for access to systems to be manipulated, which would be unlikely to be detected in a timely manner.

Finally, the escalation route from cyber issues/risks being identified and assessed, to being reported to Senior Management, as the ultimate accountable body, needs to be made clearer, so that these are sufficiently visible and understood. This includes refining the Information Governance Group's purpose to devote time to IT systems issues periodically and act as the decision-making forum for escalation to the Executive Team (ELT).

Progress towards the 2022/23 Audit Plan

2.2 Since the last update to the Committee, there has been no further changes to the audits set out within the 2022/23 Audit Plan.

2.3 The table below provides a summary of progress to date (19/01/23):

Audit/ Audit follow up status	Number of reviews	%
Finalised	6	28.6
Draft report	5	23.8
In progress	7	33.3
	18	85.7%
Audits to be started Q4	3	14.3
Total	21	100%

NB: The figures within the table include 2 audits carried forward from the 2021/22 audit plan.

2.4 Currently the audit plan is on track to be completed by the end of the financial year.

4. Expected Deliverables for Q4 2022/23

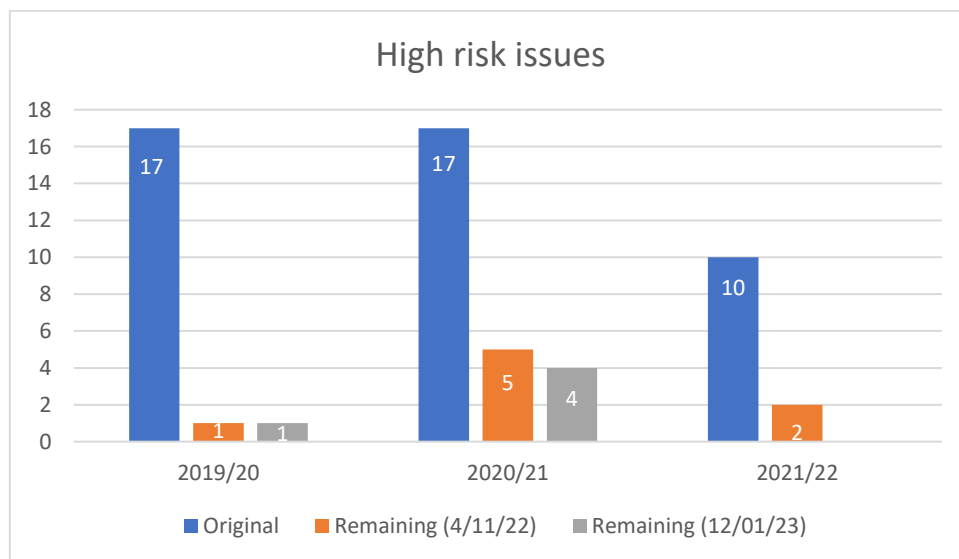
4.1 The work expected to be delivered in quarter 4 is detailed within the table below. It should be noted that 10 of these audits have already commenced with 4 at draft report stage. These audits can be subject to change due to the evolving auditing environment. Updates on these will be provide at the next committee meeting:

Service	Audit/ follow up/descriptor
HR&OD	Staff Recruitment & Retention – <i>A review over staff vacancies, especially key positions, and the measures taken to retain staff</i>
ACE	Procurement - <i>A review of the procurement process in the Council and the interaction with Portsmouth CC under the Service Level Agreement.</i>
Finance	Cash Receipting – <i>A review over key financial system</i>
Finance	Council Tax Billing, Collection & Recovery – <i>A review of Council Tax with a focus on debtors and recovery</i>
Economy, Planning and Strategic Housing	Suitable Alternative Natural Green Space (SANGS) - <i>A follow-up of the audit from 2019/20</i>
Finance	Treasury Management - <i>A review over key financial system</i>
Operations	Taxi Licensing follow up audit – <i>A follow up on the previous audit carried out.</i>
Property, Estates and Technical Services	Concerto Property System – PIR Audit – <i>A review of the implementation of the new property system.</i>

Service	Audit/ follow up/descriptor
ACE	Performance Management
ELT	CREP – <i>A review of the value for money of the investment in the development of the Council's CREP savings programme</i>
Operations	CCTV – <i>Transfer of CCTV</i>
Legal Services	Information Governance – <i>A review of the Council's information Governance framework</i>
IT Services	Application Patch Management follow up audit – <i>A follow up of the previous audit carried out.</i>
IT Services	IT Development – <i>Reviewing the IT Digital teams development work.</i>

5. Outstanding High Risk Audit Issues

5.1 The high-risk issues identified are ones which require focus by the organisation in order to implement the actions agreed to mitigate the high-risk issues identified. Below the graph shows the number of high-risk issues identified against the number implemented as of January 2023.



5.2 It is in the Audit Manager's opinion that sufficient progress is being made towards the high-risk recommendations and there is nothing to draw to the Committee's attention in relation to these.

5.3 The table below shows the expected completion date for these outstanding high risks.

Year recommendations made	Service Area	Audit	No. of high-risk recommendations	Expected implementation date	Total
2019/20	Finance/IT	PCI DSS	1	31/7/23	
					1
2020/21	IT	Application Patch Management	1	31/5/23	
2020/21	Finance	Purchase Ledger	2	28/2/23	
2020/21	ACE	Contract Management	1	31/3/23	
					4

6. Recommendation

6.1 Members are requested to note the information provided within the report in relation to the progress of Audit work to date towards the 2022/23 audit plan, the expected deliverables for Q4 and the outstanding high risk audit issues.

AUTHOR: Nikki Fleming, Audit Manager
07867 377484

nikki.fleming@rushmoor.gov.uk

HEAD OF SERVICE: Simon Little, Interim Executive Head of Financial Services and S151 Officer

References: *Internal Audit – Audit Plan 2022/23*, presented to the Committee on 28 March 2022.

[Agenda for Corporate Governance, Audit and Standards Committee on Monday, 28th March, 2022, 7.00 pm - Rushmoor Borough Council](#)