Report to the Audit and Governance Committee

Report reference:
Date of meeting: 15 July 2021

Epping Forest
District Council

Portfolio:	**Leader of the Council**	
Subject:	**Internal Audit Monitoring Report July 2021**	
Responsible Officer:	**Sarah Marsh**	**(01992 564446).**
Democratic Services:	**Laura Kirman**	**(01992564723)**

Recommendations/Decisions Required:

(1) The Committee notes the summary of the work of Internal Audit and the Corporate Fraud Team for the period March to July 2021

(2) Agrees the scope of the External Quality Assessment of the Internal Audit service

Executive Summary:

This report updates Members on the work completed by Internal Audit and the Corporate Fraud Team since the March 2021 Audit and Governance Committee and provides the current position in relation to overdue recommendations.

The report sets out the scope of the External Quality Assessment of the Internal Audit Service which is required by the Public Sector Internal Audit Standards to be undertaken every five year; the last one being 2016.

Reasons for Proposed Decision:

Monitoring report as required by the Audit and Governance Committee Terms of Reference.

Other Options for Action:

No other options.

Report:

2020/21 Internal Audit Plan

1. The audit plan for 2020/21 is almost complete and sufficient work has been undertaken in order for the Chief Internal Auditor to give their annual report and assurance opinion which is reported elsewhere in the agenda. Progress is being made on the 2021/22 Audit Plan as detailed in Appendix 1.

2. The following six final reports have been issued since the Committee received its last update in March 2021.

Qualis Group Governance (substantial assurance)

Model Articles of Association and a Shareholder Agreement, setting out the reserved matters, are in place for the Qualis Group. The extent to which the S151 Officer, as the Shareholder's Representative, is authorised to make decisions on behalf of the Council is set out in writing in a Cabinet report. To provide greater clarity and ensure compliance with the Shareholder Agreement, a delegation matrix distinguishing responsibility and accountability between the Council (as shareholder), Qualis Board and directors should be prepared.

The permanent Qualis Board has been in place since October 2020 and comprises suitably experienced and skilled members. Appointments were approved by Full Council following recommendation by the Council's Senior Management Selection Panel. Conflicts of Interest are appropriately managed and to provide additional transparency a conflicts register is being introduced and will be in place by end of July 2021.

Qualis Group 2020/21 one-year business plan has been approved by Cabinet, but the four-year plan was not presented until later in the year as the Board was developing its medium-term strategy. As part of a wider piece of work, a review of the information to be included in the Business Cases for future transfer of services is being carried out by the Council which will ensure enough relevant financial and other business measures, including the use of targets or Key Performance Indicators, are reported on to enable the Council to effectively monitor progress. To ensure the Council is aware of Qualis risks which may have a direct impact on Council risks, significant Qualis risks will be shared with the Council's Section 151 Officer to be captured as part of the Council's risk management framework.

Loans have been provided to Qualis and these have been signed, sealed and include any relevant covenants. Repayments by Qualis have been made on time and in full. The loan agreement in respect of the working capital loan was not in place before the first utilisation in January 2020; however, the Council has ensured that all subsequent loan agreements are in place before commencement to provide a legal basis for the terms of the loan.

Accounts Payable (moderate assurance)

Overall, the Accounts Payable control framework is effective and no reductions in control effectiveness have occurred due to remote working. The Council has detailed and appropriate policies and procedures to ensure that goods and services procured are required and represent best value. The Council's Procurement Rules have been recently updated and training provided to teams across the Council. A review and update of Financial Regulations, which have not been revised since 2015, is scheduled for later in 2021/22.

There are documented financial levels of delegated authority, which are complied with for order authorisation and certification of payments and there is a good segregation of duties between:

- Purchase Order origination and approval;
- Ordering processes and payments operations;
- Payment run preparation and approval to make the payments; and
- The setting up and review of new supplier details.

During 2021/22 management information reports will be developed to cover areas such as aged creditor listings, disputed invoices, suspected duplicate payments and supplier master file changes. This work was delayed from 2020/21 as resources were diverted due to changes in processes as a result of remote working and additional payment runs for Covid-19 related grants.

Active Directory Management (moderate assurance)

Active Directory management is a directory service developed by Microsoft for the administration of all PCs and servers on a Windows domain. Examination of Active Directory (AD) security settings confirmed that password ageing, complexity and minimum length had all been invoked together with robust restrictions on failed login attempts. However, testing identified that some password settings within the AD domain did not meet recommended best practice standards which increases the risk of password reuse.

A review of AD user access rights highlighted the failure to disable all inactive or unused accounts. To reduce the risk of unauthorised access to the live Council network domain, all inactive and redundant accounts have now been disabled.

Vendor support for Microsoft Windows Server 2008 ceased in January 2020 meaning that no further security patches are provided by the software vendor to address newly identified vulnerabilities. The audit identified 42 Windows Server 2008 servers running, for example, Payroll and the Academy Revenue and Benefits system. The Council is already aware of this issue and a project to remove unsupported servers is underway.

Audit policies within the AD are enabled to capture key events including user logon (success/failure), object access, changes to AD policy settings and use of superuser accounts. All information captured by selected Audit Policies is stored in the AD security log. To meet Microsoft best practice and prevent audit logs being overwritten, the size of the AD Security Log has now been increased.

Health & Safety - Council buildings and depots (moderate assurance)

At a Corporate level the Council has a Health and Safety Policy, and this is underpinned by other policies relevant to this audit, for example an Asbestos Policy and a Water Quality Policy. There is, however, no policy or associated procedures that define the Health and Safety framework at the Council's offices and depots and responsibility is assigned across multiple officers. As a result, there is no single record to cover the following which could result in a compliance issue not being scheduled in accordance with guidance or an action not be followed up and cleared:

- Recording of all compliance testing, checking servicing and risk assessments to cover all Council sites; and
- Recording and logging of all actions, matters arising and the deadlines for implementation at each site.

Governance would be enhanced through quarterly exception reporting to the Corporate Safety Team covering depots and offices detailing any overdue compliance testing and certification and flagging up recommended actions and matters that have exceeded their designated implementation date.

Storage Area Network (limited assurance)

The Storage Area Network (SAN) is a dedicated network for data storage. In addition to storing data, SANs allow for the automatic backup of data, and the monitoring of the storage and the backup processes. SAN hardware is located in a secure ICT server room and access is restricted to a small number of ICT technical support staff. ICT are in the process of reviewing current swipe card access rights and going forward will regularly review and validate access to the server room to ensure it is minimised.

SAN hardware is afforded full environmental protection including fire suppression, air conditioning and Uninterruptible Power Supply (UPS), and these systems are subject to regular service and testing. The SAN platform is patched up to date and monitoring software is installed to manage both system performance and generate real time alerts in the event of system downtime.

A separate WatchGuard firewall appliance provides enhanced network security. However, as the WatchGuard appliance is out of vendor support and has not been patched since 2016, ICT are in the process of replacing the firewall hardware protecting the SAN infrastructure. The firewall appliance is administered via a single 'admin' account. To prevent unauthorised access, individual user accounts will be assigned to all firewall administrators and robust firewall appliance password policies will be enabled.

The SAN is centrally administered via a DataCore Management Console which system administrators log on to via a shared default 'Administrator' account. No policy was enabled to enforce password security settings including ageing, complexity, history or minimum length on the Administrator account. ICT have agreed that all SAN administrators will be assigned individual logon credentials and access controls will be enhanced.

The IT service is currently working with the IT auditor on how best to resolve the issues raised in an expedient manner.

IT Disaster Recovery (Limited assurance)

Extensive work has been undertaken by IT to design and implement a robust IT Disaster Recovery (DR) solution to safeguard Council systems. A third party has been contracted to provide a cloud based secondary data centre DR facility meaning all Council systems should be restored within a two-hours. A full DR test is scheduled for later in the year to provide evidence-based information about the efficacy of, and the likely elapsed times for, partial or full restoration of Council critical systems.

The Disaster Recovery facility does not include any of the Council's legacy applications as these reside on physical servers. These systems are likely to be more time consuming and difficult to recover in the event of a DR situation. An Application Strategy is being drafted outlining timescales for the replacement of all remaining legacy systems.

A documented IT Disaster Recovery plan will be produced outlining all key stages to recover the Council's IT infrastructure to ensure there is a structured approach to any recovery action or system rebuilding / data restore processes that might be necessary. This will expedite system recovery and reduce any unnecessary downtime.

Going forward, Disaster Recovery arrangements will be regularly tested, and a Post Recovery Review process put in place to ensure each ITDR test is subject to critical evaluation. This will include any service affecting issues (near misses) that can be incorporated into the lessons learnt process. IT Disaster Recovery plans will be reviewed and updated following both recovery tests and significant service affecting issues to ensure that valuable information or opportunities to enhance processes are captured.

Recommendation Tracker

3. The Audit and Governance Committee continues to receive details of all overdue recommendations, plus any high priority recommendations from final reports regardless of whether they are overdue or not.

4. The current tracker is shown at Appendix 2 and contains two high and five medium priority recommendations which have passed their due date and two high priority

recommendations not yet due.

5. The two overdue high priority recommendations concern replacement of the Storage Area Network (SAN) firewall to provide a fully vendor supported firewall appliance and implementation of new policies and accounts on the new firewall. This has been delayed due to IT equipment shortages in the UK. The risk to the Council is reduced as there is no direct connectivity to Council data through the firewall; it only allows access to the management console.

Table 1. Summary of tracker as at July 2021.

Recommendation type	Number (July 2021)	Number (March 2021)	Number (January 2021)	Number (December 2020)	Number (September 2020)
High Priority not passed its due date	2	0	0	0	0
High Priority passed its due date	2	0	1	1	2
Medium Priority passed its due date	5	1	2	2	1
Low Priority passed its due date	0	0	0	0	5
Total	**9**	**1**	**3**	**3**	**8**

Other Internal Audit activities

6. Internal Audit has continued to provide advice and guidance in several business areas:

Covid-19 central government grants for businesses: Internal Audit and the Corporate Fraud Team continue in providing advice and assistance on all the business grants schemes. This includes performing pre-award checks using the Cabinet Office due diligence tool, spotlight. and assisting with the post payment assurance verification process required by the Department for Business, Energy and Industrial Strategy.

Corporate purchase cards: Internal Audit is facilitating discussions on the Council’s approach to the use of purchase cards which are being considered to streamline the processes for low level spend and one-off payments. Input is provided around achieving value for money whilst retaining adequate controls.

Supplier payment processes: Advice is being provided around supplier payment processes, primarily to prevent the Council incurring late payment charges from suppliers, but also to review current processes to identify efficiencies.

Information Governance: Internal Audit is actively involved in both the Strategic Information Governance Group (SIGG) and the operational Information Asset Owners Group, feeding back to the Corporate Governance Group. Internal Audit resource is being provided to help deliver the SIGG work plan, including a review of current information governance policies, compliance with the Transparency Code 2015 and the use of Data Protection Impact Assessments in project management.

Service Assurance Statements: Internal Audit completed the annual service assurance exercise consulting with Service Managers and Service Directors as part of the annual governance process, to provide assurance to the Council and its stakeholders that good governance arrangements are in place. The results have been fed into the Annual Governance Statement.

National Fraud Initiative (NFI) 2020/21: Internal Audit coordinated preparations for the 2020/21 NFI exercise, including the new Covid Grant Recipient's dataset. The review of matches is in progress.

External Quality Assessment (EQA)

7. In line with the Public Sector Internal Audit Standards (PSIAS) an external assessment of the Internal Audit function needs to be undertaken at least once every five years by a qualified independent assessor from outside the Council. The form of the external assessment and the qualifications and independence of the external assessor, including any potential conflict interest, must be discussed with the Audit Committee.

8. The last EQA was undertaken in 2016/17, the results of which were reported to the March 2017 Audit and Governance Committee meeting. The EQA concluded the Internal Audit function was compliant with the PSIAS and it compared favourably with regards to its peers both within local government and the wider industry.

9. The EQA may be accomplished through a full external assessment, or a self-assessment with independent external validation. Like last time the EQA will be achieved through the self-assessment route.

10. Following a tender process Gard Consultancy Services (GCS) has been appointed to undertake the EQA in July 2021. The results of which will be reported to the September 2021 Audit and Governance Committee. Fieldwork will include interviews with the Audit Chairs of Harlow, Broxbourne and Epping Forest as well as each Section 151 Officer.

11. GCS's managing director, Ray Gard, will be undertaking the review and is an experienced finance and governance manager with extensive public sector experience. His last role being Assistant Director of Finance – Audit, Fraud and Risk Management at London Borough of Waltham Forest (2010-2016). There are no potential conflicts of interest between GCS with the Chief Internal Auditor or Harlow, Broxbourne and Epping Forest Councils.

Corporate Fraud Team (CFT) update

12. Since March a further four Right to Buy's (RTB) have withdrawn following their vetting interviews by the team. Another RTB was cancelled after a year long investigation into the validity of the funding whereby it was confirmed that the applicant had been gifted monies from her partner who was found to have abused the Power of Attorney status they hold over their elderly father's finances. Another application along similar lines is currently being investigated. The team has also successfully stopped two tenancy successions.

13. Work has begun on investigating the NFI matches as well as preliminary work on several proactive data mining exercises that will be taking place over the coming months.

14. The Corporate Fraud Team Manager took part in the second Webinar for the public hosted by the housing team in which the work of the CFT was promoted and included an awareness session on social housing fraud.

Legal and Governance Implications:

None

Safer, Cleaner and Greener Implications:

None

Consultation Undertaken:

Corporate Governance Group

Background Papers:

2021/22 Audit Strategy and Plan

Risk Management:

Failure to achieve the audit plan and poor follow up of audit recommendations may lead to a lack of assurance that internal controls are effective and risks properly managed, which ultimately feeds into the Annual Governance Statement.

Equality Analysis:

The Equality Act 2010 requires that the Public Sector Equality Duty is actively applied in decision-making. This means that the equality information provided to accompany this report is essential reading for all members involved in the consideration of this report. The equality information is provided at Appendix 3 to the report.