

# **NORTH YORKSHIRE COUNTY COUNCIL**

## **AUDIT COMMITTEE**

**12 DECEMBER 2022**

### **INTERNAL AUDIT REPORT ON INFORMATION TECHNOLOGY, CORPORATE THEMES AND CONTRACTS**

#### **Report of the Head of Internal Audit**

#### **1.0 PURPOSE OF THE REPORT**

- 1.1 To inform Members of the internal audit work completed during the year to 30 November 2022, in respect of information technology (IT), corporate themes, and contracts and procurement.

#### **2.0 BACKGROUND**

- 2.1 The Audit Committee is required to assess the quality and effectiveness of the corporate governance arrangements operating within the County Council. In respect of IT, corporate themes and contracts, the Committee receives assurance through the work of internal audit (provided by Veritau) as well as relevant update reports from officers.
- 2.2 This report considers the work carried out by Veritau during the year to 30 November 2022. It should be noted that the internal audit work referred to in this report tends to be cross cutting in nature and therefore there are no corresponding directorate risk registers to consider.

#### **3.0 WORK CARRIED OUT DURING THE YEAR TO 30 NOVEMBER 2022**

- 3.1 Summaries of the internal audit work undertaken and the reports issued in the year are attached as follows:

IT audit assurance and related work	<b>Appendix 1</b>
Corporate assurance	<b>Appendix 2</b>
Contracts and procurement	<b>Appendix 3</b>

- 3.2 Veritau has also been involved in a number of related areas, including:

- providing advice on corporate governance arrangements and IT related controls;
- providing ongoing advice and support to various corporate / project groups; including the Supply Chain Resilience Board, Contracting Project Board and the LGR Finance Procurement sub-group.
- providing advice and guidance to directorates and schools on ad hoc contract queries and on matters of compliance with the County Council's Contract and LMS Procedure Rules;

- carrying out investigations into corporate or contract related matters that have either been communicated via the Whistleblowers' hotline or have arisen from issues and concerns reported to Veritau by management.
- 3.3 In addition to the IT audits detailed in **appendix 1**, there has been coverage of IT related controls and activities as part of general audits where key IT systems are in operation. As part of directorate based plans, audit work has also covered procurement and/or contract related matters.
- 3.4 As with previous audit reports an overall opinion has been given for each of the specific systems or areas under review. The opinion given has been based on an assessment of the risks associated with any weaknesses in control identified. Where weaknesses are identified then remedial actions will be agreed with management. Each agreed action has been given a priority ranking. The opinions and priority rankings used by Veritau are detailed in **appendix 4**. Where the audits undertaken focused on systems development, the review of specific risks as requested by management or value for money then no audit opinion has been given. The work completed and the opinions given following each audit contribute to the annual report and opinion of the Head of Internal Audit.
- 3.5 It is important that agreed actions are formally followed up to ensure that they have been implemented. Veritau follow up all agreed actions on a regular basis, taking account of the timescales previously agreed with management for implementation. On the basis of the follow up work undertaken during the year, the Head of Internal Audit is satisfied with the progress that has been made by management to implement previously agreed actions necessary to address identified control weaknesses.

#### 4.0 **RECOMMENDATION**

- 4.1 That Members note the results of internal audit work performed in the period in respect of the Council's information technology, corporate and contract arrangements.

Max Thomas  
Head of Internal Audit

Veritau Ltd  
County Hall  
Northallerton

25 November 2022

## **BACKGROUND DOCUMENTS**

Relevant audit reports kept by Veritau.

Report prepared by Stuart Cutts, Assistant Director – Audit Assurance, Veritau and presented by Max Thomas, Head of Internal Audit, Veritau

## APPENDIX 1

### INFORMATION TECHNOLOGY - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 30 NOVEMBER 2022

	System/ Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	ICT Capacity Management	Substantial Assurance	<p>ICT Capacity Management is the planning and monitoring of network resources to ensure the Council's network and key systems are always available to end users.</p> <p>The purpose of this audit was to review whether the Council:</p> <ul style="list-style-type: none"> <li>• has a capacity management plan in line with relevant ISO requirements</li> <li>• monitors and analyses relevant information and data to predict and support future requirements</li> <li>• planning meets the capacity requirements for the Council</li> </ul>	June 2022	<p>An ICT Capacity Management Plan is in place and covers all the key areas outlined within ISO 20000 (the international standard for ICT service management).</p> <p>This plan includes assessing the current and future demands of ICT services, the expected impact of agreed requirements for availability and service continuity, and the impact of organisational changes and new technologies.</p> <p>Tools are in place to monitor usage. IT usage can also be monitored at the Councils individual sites. Technology and Change work closely with their suppliers who also monitor internet usage and alert the council to any issues.</p>	<b>No actions identified.</b>

System/ Area		Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					The Councils internet bandwidth meets the needs of the users.	
B	Symology	Limited Assurance	<p>The Symology system supports the management of highways assets, street lighting and street works.</p> <p>The purpose of this audit was to ensure that:</p> <ul style="list-style-type: none"> <li>access to the Symology system was restricted to authorised individuals</li> <li>the system was secure</li> <li>the development and maintenance of the system was in line with ISO requirements</li> <li>the management of the system conformed with performance management set out in ISO 20000.</li> </ul>	July 2022	<p>Processes and procedures ensure only authorised users have access to Symology.</p> <p>Access controls are monitored by the system administrator. There is a secure connection to log on to the Symology system.</p> <p>A number of improvements to password requirements and controls were recommended.</p> <p>Symology is a business-critical system for NYCC and NY Highways. However, there was no written strategy for how the system should be developed in the immediate future.</p> <p>The Council has a corporate access control policy in line with ISO 27001. That policy requires each system to have their own access control policy. There is currently no access control policy for Symology.</p>	<p><b>Four Priority 2 and Five Priority 3 actions were agreed</b></p> <p><b>Responsible Officer(s):</b> Head of Central Systems Team, Corporate Systems Service Owner, and Systems Development Officer (Business)</p> <p>Management and system governance arrangements have been moved to Technology and Change (T&amp;C). A Service Level Agreement is now place with BES.</p> <p>All changes to Symology are now approved by the T&amp;C change management processes.</p> <p>A number of other actions are planned to address the remaining areas for</p>

System/ Area		Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
					<p>There is a change management policy in place which covers all areas recommended by ISO 27001. However, currently there is no log of changes made to Symology. Consequently, we were unable to confirm that all changes to Symology are authorised, tested, logged and completed within a reasonable timescale.</p> <p>Third party assurances on Symology system security have also not been obtained.</p>	improvement. The current timescale to complete all remaining actions is by the end of April 2023.
C	Cyber Readiness	Substantial Assurance	<p>Cyber security remains a significant risk area for all public bodies. The government has rated 'cyber attacks' as one of the top four risks to UK National Security.</p> <p>The purpose of this audit was to review whether:</p>	November 2022	<p>The Council's disaster recovery planning is up-to-date and includes all key areas as recommended by ISO 27002.</p> <p>Policies are in place setting out the different types of backups required for different network components and systems, as well as frequency and retention periods. Backups were being taken in accordance with the policy. There is also a procedure</p>	<p><b>Three P3 actions were agreed</b></p> <p><b>Responsible Officer:</b> Various</p> <p>All back-ups are now encrypted and are stored in locations with restricted access. Relevant changes to standing operating procedures have been made.</p>

	System/ Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			<ul style="list-style-type: none"> <li>plans are in place to respond to a cyber-attack</li> <li>key systems and data can be restored following a cyber-attack within the council's recovery point and recovery time objective</li> <li>Technology &amp; Change provide assistance to service areas to prepare for a cyber-attack.</li> </ul>		<p>to monitor and ensure backups are completed successfully.</p> <p>Backups were stored in secure locations at multiple different sites, increasing the security of, and resilience for, restoring data.</p> <p>Backups were not being encrypted; which is recommended by ISO 27002. We noted a small number of instances where the Council's standard operating procedures were not being followed.</p> <p>The Council's business continuity impact assessments and business continuity plans had not been reviewed by Technology and Change (T&amp;C) to verify that the expectations of service areas was in line with T&amp;C capabilities.</p>	<p>T&amp;C are currently reviewing the business continuity requirements (coordinated by the Emergency Planning Team) with backup methods to identify whether there are any gaps. This work is planned to be completed by the end of 2022.</p>

## APPENDIX 2

### CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 30 NOVEMBER 2022

	System/ Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Payroll	Substantial Opinion	<p>The purpose of this audit was to provide assurance that:</p> <ul style="list-style-type: none"> <li>the process for posting salaries was working correctly so that salary costs were coded accurately and to the right code in the general ledger</li> <li>allowances and additional hours paid to staff were appropriate and were authorised, calculated and paid correctly</li> <li>changes to bank details were carried out appropriately.</li> </ul>	May 2022	<p>A suitable process was in place for posting salaries to the correct cost codes and this was working accurately in those cases tested.</p> <p>For the claims tested which were processed either via email to Employment Support Services (ESS) or through MyView, each allowance was in line with the jobs description and had the appropriate authorisation from the employee's line manager.</p> <p>Some claims were being authorised that contained insufficient information to allow for effective checking. There is also limited guidance on the level of detail to include or the areas to check in the Council's policies.</p> <p>We found no issues with the changes to bank details reviewed.</p>	<p><b>One P3 actions were agreed</b></p> <p><b>Responsible Officer:</b> Assistant Chief Executive (Business Support)</p> <p>Reminder notes were to be sent managers regarding what their teams should be including in forms and what they should be looking for.</p> <p>Additional information and training will be provided to new managers. Officers will also undertake a full refresh of guidance for managers as part preparing for Local Government Reorganisation (LGR).</p>

## APPENDIX 3

### CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE YEAR TO 30 NOVEMBER 2022

	System/ Area	Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
A	Contract Waivers	Reasonable Assurance	<p>Contract exemption requests are completed where it is not possible to fully comply with Procurement and Contract Procedure Rules (PCPRs). In these situations, rules can be waived subject to certain criteria and only after suitable challenge and authorisation.</p> <p>The purpose of the audit was to assess whether:</p> <ul style="list-style-type: none"> <li>exemption requests were completed and authorised in line with the Procurement and Contract Procedure Rules</li> <li>best value forms were completed and</li> </ul>	November 2022	<p>Clear rules regarding which officers can provide authorisation are in place. However, guidance on how authorisation should be documented and saved is not clearly defined. Consequently, there was a lack of consistency for how/where to document authorisation evidence.</p> <p>There was supporting information indicating that correct authorisation had been obtained in all, but one case tested.</p> <p>Waivers and decision records (DRs) are not being published to Contracts Finder or Contracts Register as required by the PCPRs.</p> <p>The process to complete best value forms appeared appropriate. However, in one instance, contracts were noted</p>	<p><b>Three Priority 2 and One Priority 3 actions were agreed</b></p> <p><b>Responsible Officer:</b> Head of Procurement and Contract Management</p> <p>A standard procedure will be agreed regarding documenting and saving authorisation emails. An online signing system will also be considered.</p> <p>The Category Procurement Support Officers (CPSOs) will publish waivers and DRs going forward.</p> <p>An escalation process will be introduced for the CPSOs in the event that a best value request is believed to be non-compliant.</p>



System/ Area		Audit Opinion	Areas Reviewed	Date Issued	Comments	Action Taken
			<p>authorised appropriately</p> <ul style="list-style-type: none"> <li>adequate arrangements were in place to ensure exemptions were monitored and appropriate records were maintained of exemptions granted.</li> </ul>		<p>which were in excess of best value thresholds when combined.</p> <p>Registers are in place to record exemptions and officers have been assigned to oversee this. However, the process is largely reliant on manual input and the use of spreadsheets and forms. We also saw some inaccuracies on the registers.</p>	<p>The Senior Category Managers will be reminded of the importance of accurate record-keeping. Quarterly dip sampling will be undertaken to check the accuracy of recorded information.</p> <p>Various timescales have been agreed for the actions. All are due for completion by September 2023.</p>

## AUDIT OPINIONS AND PRIORITIES FOR ACTIONS

Audit Opinions	
Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of audit.	
Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.