

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

26 OCTOBER 2020

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 period from 1 September 2019 to 30 September 2020 in respect of information technology (IT), corporate themes and contracts.

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 relation to IT, corporate themes and contracts, the Committee receives assurance through the work of internal audit (provided by Veritau) as well as receiving copies of relevant corporate and directorate risk registers.
- 2.2 This report considers the work carried out by Veritau during the period to 30 September 2020. It should be noted 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 13 MONTH PERIOD TO 30 SEPTEMBER 2020

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

| | |
|-------------------------------------|-------------------|
| IT audit assurance and related work | Appendix 1 |
| Corporate assurance | Appendix 2 |
| Contracts and procurement | Appendix 3 |

- 3.2 Internal Audit has also been involved in a number of related areas, including:
- providing advice on corporate governance arrangements and IT related controls;
 - providing advice and support to assist various project groups;
 - 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;

- contributing to the development and roll-out of the procurement strategic action plan, including participation in a number of delivery areas;
- reviewing processes and procedures in place within property services for managing the responsive repairs contract;
- carrying out a number of 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.
- supporting the council in Covid-19 related activities, including attendance at the supplier relief resilience board and providing guidance and support on individual cases.

3.3 In addition to the specific IT audits detailed in Appendix 1, there has been an increased 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 there have also been a number of reviews which include 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**.

3.5 It is important that agreed actions are formally followed up to ensure that they have been implemented. Veritau formally 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.**

3.6 The programme of audit work is risk based. Areas that are assessed as well controlled or low risk tend to be reviewed less often with audit work instead focused on the areas of highest risk. Veritau's auditors work closely with directorate senior managers to address any areas of concern.

4.0 **RECOMMENDATION**

4.1 That Members consider the information provided in this report and determine whether they are satisfied that the internal control environment operating in respect of information technology, corporate and contract arrangements is both adequate and effective.

Max Thomas
Head of Internal Audit

Veritau Ltd
County Hall
Northallerton

26 October 2020

BACKGROUND DOCUMENTS

Relevant audit reports kept by Veritau Ltd at 50 South Parade, Northallerton.

Report prepared and presented by Max Thomas, Head of Internal Audit (Veritau).

INFORMATION TECHNOLOGY - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 30 SEPTEMBER 2020

| | System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|---|------------------------|-----------------------|---|-------------|--|--|
| A | Communication Security | Substantial Assurance | <p>Communications security ensures that message content is delivered to the intended recipients, whilst preventing unauthorised interception and access.</p> <p>The purpose of this audit was to review whether:</p> <ul style="list-style-type: none"> • accountability for the security of data during transmission had been defined • council staff had been provided with sufficient direction in security procedures, • arrangements were in place to ensure the required security configuration would be applied to email communications and other security measures, such as the checking of email authenticity, were in place and operating effectively. | June 2020 | <p>All staff are required to complete the 'data protection GDPR update' online training. Each year a highlight report is produced for all users that have not completed the training course.</p> <p>We found only one example where an email could have been sent more securely. However, the risks were minimised as data was anonymised.</p> <p>The measures in place to ensure the integrity of emails received as well as controls to prevent e-mails from being spoofed are good. The council has not applied Domain Name System security extensions as this is not provided by the councils DNS provider.</p> <p>The council's e-mails are scanned by anti-virus software. The council performs automated dynamic analysis of attachments and keeps a log of all e-mails sent and received by staff.</p> <p>The council does not whitelist file attachments which is best practice according to the National Cyber Security Centre (NCSC).</p> | <p>Two P3 actions were agreed.</p> <p>Responsible Officer: Assistant Director Technology and Change</p> <p>The council currently has a blacklist on the anti-virus software for blocking executables and Windows shortcuts that can be exploited by malware. The council has recognised that it would be more secure to develop a whitelist of applications. However it would be a challenge to identify all the file types the authority uses. The council's inclusion within the NCSC Active Defence Hub most likely negates the need for whitelisting.</p> <p>NCSC Active Defence Hub most likely negates the need for the DNSSEC. The Council's DNS is routed via the NCSC Protective DNS service, which filters malicious domains, stopping malware delivery before it reaches the council's network.</p> |

| System/Area | | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|---------------------------------------|-----------------------|--|--------------|--|---|
| B | Zellis (HR) System | Substantial Assurance | <p>The Council uses the Zellis Resourcelink (formerly Northgate Resourcelink) system to provide its payroll and human resources functions.</p> <p>The purpose of this audit was to review whether:</p> <ul style="list-style-type: none"> access to the Zellis Resourcelink system was suitably controlled and authorised an effective operational environment was in place that maintains the security, integrity and availability of information in Zellis changes to the system and incidents or problems involving Zellis are managed in accordance with established procedures | October 2019 | <p>Up to date policies and procedures regarding access to the system were in place.</p> <p>Users are provided with unique login IDs and are assigned to established user roles and security groups, which define and limit system privileges within the system. User access requests, requests for changes to accounts and requests to close accounts are recorded and handled appropriately.</p> <p>There are suitable procedures for recording, reviewing and resolving incidents and problems.</p> <p>We noted that the annual review of user accounts had not been carried out since May 2017.</p> <p>Although Zellis ResourceLink logs user activity, audit logs are not periodically produced and reviewed for unusual or unexpected activity.</p> <p>Changes requested for ResourceLink complied with the process as set out in best practice guidance.</p> | <p>Two P3 actions were agreed.</p> <p>Responsible Officers: Senior Systems Officer, Finance & HR Systems Team Leader</p> <p>A review of current user accounts will be undertaken to establish whether they are still required and whether their access rights are appropriate. Reviews will then be undertaken on an annual basis.</p> <p>Reviews of privileged user activity will be undertaken on a monthly basis with a different user or users selected each month.</p> |
| C | Service Request & Incident Management | Reasonable Assurance | Service requests are generally defined as requests for information, advice, and | August 2020 | Arrangements for the management of incidents and service requests was found to be generally good. | Two P2 and Seven P3 actions were agreed. |

| | System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|---|---------------------|-----------------------|---|-------------|---|--|
| | | | <p>access to a service or a pre-approved change. Incidents, by contrast, are unplanned interruptions to a service. An effective service request and incident management process helps to minimise the impact and duration of issues encountered by users and the organisation.</p> <p>The purpose of this audit was to review whether:</p> <ul style="list-style-type: none"> • there was an efficient and effective approach to the management of ICT-related information security incidents, including communication on security events and weaknesses (ISO 27001) • incidents and service requests were managed in an efficient and effective manner, in accordance with documented policies and procedures (ISO 20000). | | <p>Information security incidents are not classified or assigned consistently in the incident management system (Ivanti).</p> <p>An Information Security Management System (ISMS) case log and library have been established, with access restricted to authorised officers. However, some incidents recorded in the ISMS case library were not recorded on the incident case management system.</p> <p>There are arrangements in place for the handling of evidence relating to information security incidents but these had not been documented as part of the existing policy/procedure.</p> <p>Not all KPI's in existing policies for incidents and service requests are reported on. Performance has also declined for incident resolution.</p> <p>There is not a clear distinction between major and high priority incident criteria.</p> | <p>Responsible Officers: Security Information Security Compliance Officer, Service Manager – Corporate Systems, Service Desk Team Leader and Service Management Office Lead Analyst.</p> <p>The Technology & Change Directorate currently has an ITSM project to improve service management arrangements and implement a new version of the incident management system (Ivanti). It is expected a number of the findings raised in this work will be resolved through the project.</p> <p>Security incident categorisation and assignment will be clarified as part of the project. The ITSM policy review will be completed and revised policies approved. Training will be provided to staff on the revised policies and procedures.</p> <p>KPIs for incident and service request management will be reviewed. Performance will be managed through the Service Management Improvement Plan.</p> |
| D | Supplier Management | Substantial Assurance | The council uses a number of different systems for a wide | August 2020 | Processes and procedures were in line with the requirements of ISO | One P3 action was agreed. |

| System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|---------------|--|-------------|---|---|
| | | <p>range of critical functions. They store a significant amount of data and in many cases the data is sensitive. It is critical the data is always available. External suppliers provide many of these key systems. However it is the council's responsibility to ensure the systems are delivering a high quality of service.</p> <p>The purpose of this audit was to review whether:</p> <ul style="list-style-type: none"> the council and their systems service providers had a robust contract in place in line with the control requirements of ISO 20000 and ISO 27001 the corporate systems team adequately reviews performance of the systems service provider to ensure it is in line with contract obligations. | | <p>20000 and 27001 for the management of suppliers.</p> <p>The majority of contracts reviewed conformed to the required clauses. The contracts that did not contain all the required clauses are undergoing a retender exercise using the G-Cloud framework.</p> <p>The contracts contained a clear performance framework that was documented and agreed with clients. Clear procedures ensured that the suppliers were meeting the required needs of the service area. Where the supplier was not meeting the needs of the service, the systems team took appropriate action.</p> <p>All systems that contained a high volume of special category data are hosted on the council's network. For systems hosted remotely, the council obtains assurance from the supplier that strict data security policies are in place, the council's data is secure and the suppliers host the data securely. The supplier questionnaire could be further improved by asking questions concerning Web Application/Website Security and Standards.</p> | <p>Responsible Officer: Service Manager - Corporate Systems Team</p> <p>Technology and Change technical standards will be reviewed to ensure that hosted systems are secure. As part of this review Technology and Change will consider adhering to best practice guidance relating to Web Application/Website Security and Standards.</p> |

CORPORATE THEMES - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 30 SEPTEMBER 2020

| | System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|---|------------------------|----------------|--|---------------|---|--|
| A | Commercial Investments | High Assurance | <p>Commercial Investments are governed by a number of statutory and good practice requirements. We reviewed the current arrangements to ensure:</p> <ul style="list-style-type: none"> robust due diligence arrangements are in place for all investments effective risk management arrangements exist for all potential investments the Council is complying with the CIPFA Prudential Code, and the associated update relating to commercial investments. | February 2020 | <p>Appropriate processes and controls were in place for commercial property investments including undertaking financial and market due diligence. These processes and controls sought to highlight any potential financial, or market based issues prior to the investment being made.</p> <p>There is appropriate delegated authority in place for investment decisions, which was followed in the commercial property investments we reviewed.</p> <p>The CIPFA Prudential Code highlights the importance of ensuring commercial investment is linked to Council objectives. Investment return is clearly highlighted within the Council's budget strategy and the medium term financial plan. This income helps the Council to support service delivery by addressing the savings gap and building resilience.</p> <p>It was noted that there is currently no commercial risk register, or a document outlining specific risks for individual investments.</p> | <p>One P3 action was agreed. Responsible Officer: Corporate Director Strategic Resources.</p> <p>Risks are documented in the business cases to support investment decisions and are subject to active management where necessary. However, the on-going management of those risks will be more clearly documented through the Commercial Investment Board meeting notes.</p> <p>The on-going management of the strategic risks to the overall framework will now be reported to the Commercial Investment Board on a quarterly basis.</p> |

| System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|---|---|--------------|---|---|
| B | Customer compliments and complaints (HAS) | <p>The purpose of this audit was to provide assurance that complaints were;</p> <ul style="list-style-type: none"> • effectively recorded • dealt with in line with both legislative and Local Government and Social Care Ombudsman (LGSCO) requirements • fully investigated and supported by appropriate responses to the complainants • reviewed to identify areas for improvement that could then be used in future case management. <p>This audit focused on complaints within the Health and Adult Services Directorate (HAS) who had recently reviewed and updated their procedures.</p> | October 2019 | <p>10 complaint cases were reviewed and no issues identified. All were referred to appropriate staff for investigation, Delay letters were sent out proactively.</p> <p>The complaints team were informing the LGSCO of any potential delays promptly.</p> <p>Some improvements were highlighted. A number of response letters were of low quality and lack consistency. 'Lessons learnt' from individual cases were also not being sufficiently documented or tracked. A number of cases on the iCasework system were found to be outstanding.</p> <p>Two separate systems were being used to track complaints whereas only one system is required.</p> <p>No records are being maintained on the authority's case management system, Liquid Logic (LLA). This means that there is nothing to cross reference from the LLA care management system back to iCasework.</p> <p>Some public-facing documentation is not Care Act compliant or regularly updated.</p> | <p>Five P3 actions were agreed.</p> <p>Responsible Officers; Governance Manager & Customer Response Manager</p> <p>Poor quality complaints will be escalated. The new system for responses has already seen improvements. Work will be done with technical officers to see what improvements can be made with LLA and iCasework. Criteria will also be developed around the recording of improvements identified.</p> <p>From 1 October 2019 only one system will be used to track complaints.</p> <p>The Complaints Team has attended the HAS Leadership Forum to present on the importance of complaints and provide guidance.</p> <p>A working group is reviewing and updating the public facing documentation and toolkit for teams. A toolkit for providers is also being developed.</p> |

| System/Area | | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|------------------|-----------------------|--|----------------|---|--|
| C | Payroll/HR | High Assurance | <p>From April 2019 there was a change to the NJC terms and conditions resulting in a new pay and grading structure being introduced. Increments for the year had to be processed prior to the new structure being implemented to ensure staff were on the correct grade at the start of the new-year.</p> <p>The purpose of this audit was to provide assurance that:</p> <ul style="list-style-type: none"> • changes to the grading system had been applied correctly • increments were correctly calculated and paid only to employees who qualified • leavers were processed in accordance with the correct procedures. | October 2019 | <p>Processes used for making changes to the grading system appeared appropriate and effective. A record was maintained of those that had been checked as part of this process.</p> <p>We undertook a full review of the data from ResourceLink. No issues were identified.</p> <p>Where increments had been paid we identified no issues with the sample reviewed. Where they had not been paid, appropriate evidence to justify this was provided by ESS.</p> <p>The Leaver's Policy and Procedure was not always being followed. Some managers had not uploaded all relevant documentation onto the HR records management system (Wisdom). There was not always supporting information on Wisdom to evidence the fact that leavers' interviews had taken place. The current policy does not state where completed questionnaires should be saved.</p> | <p>One P3 action was agreed.</p> <p>Responsible Officers; Head of Employment Support Service.</p> <p>The leaver's workflow will be looked at as part of a project that is currently underway and will look at making managers responsibilities clearer and the process easier for managers all in one place.</p> |
| D | Savings Delivery | Substantial Assurance | The audit reviewed three savings proposals across CYPS: Special Educational Needs (SEN), Disabled Children and | September 2020 | Savings in the School Improvement Service and savings attached to the transformation of the PRS/AP in SEN have been managed as part of the 2020 process. We found that all | <p>One P3 action was agreed.</p> <p>Responsible Officer: Assistant Director – Strategic Resources and Assistant Director Inclusion.</p> |

| System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|--|---|----------------|--|---|
| | | <p>Young People's Service, and School Improvement.</p> <p>The purpose of this audit was to provide assurance that:</p> <ul style="list-style-type: none"> • savings plans were effective and appropriate • monitoring and reporting arrangements regarding savings progress were sufficient • savings targets had been achieved and future targets were obtainable | | <p>necessary documentation had been completed as required by the guidance. There was adequate evidence to support the savings in the School Improvement Service. The project is now closed, with savings realised on 1 January 2020. There was adequate evidence to support the transformation of the PRS/APS, and the related savings calculations. The proposal is on course to achieve its saving target.</p> <p>The Disabled Children and Young People's Service is unlikely to achieve the initial savings target of £470k. We were not provided with a risk register or action plan, and the project management methodology had not been followed.</p> <p>All the projects were being monitored and reported adequately through project boards/implementation groups, CYPLT and Executive.</p> | <p>A strategic review of Disabled Children's Services is being commissioned and scoped and will be undertaken during financial year 2020/21. The delivery and implementation of any actions or recommendations will follow the robust programme and project management principles and processes adopted by the rest of the Directorate.</p> |
| E | <p>Information Security compliance audits</p> <p>2x High Assurance</p> | <p>Various compliance visits:</p> <ul style="list-style-type: none"> • 1 Racecourse Lane • Castle House • Crayke House • Legal | <p>Various</p> | <p>Following each visit, a detailed report was sent to the Senior Information Risk Owner (SIRO), as well as to relevant directorate managers.</p> <p>Data security practices and compliance with council policies was found to be poor in a number of instances.</p> | <p>Four P2 and Three P3 actions were agreed.</p> <p>Responsible Officers: various</p> <p>Responses have been obtained from relevant directorate managers following each audit. The findings</p> |

| System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|--|--|-------------|----------|--|
| | 3x Substantial Assurance 4x Limited Assurance | <ul style="list-style-type: none"> • Morton on Swale • North Block • South Block • The Village • White Rose House | | | have been taken seriously and management has taken immediate action where issues have been discovered. |

CONTRACTS - FINAL AUDIT REPORTS ISSUED IN THE PERIOD TO 30 SEPTEMBER 2020

| | System/Area | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|---|------------------------------|------------------|--|-------------|--|--|
| A | Responsive Repairs follow up | No opinion given | <p>An unannounced follow up visit was carried out in July 2019.</p> <p>The purpose of this review was to determine if procedures implemented to address the weaknesses highlighted in the December 2018 audit report were continuing to operate effectively.</p> <p>Work was also done to establish if appropriate progress had been made to resolve issues still outstanding in March 2019.</p> | July 2020 | <p>Good progress has been made by Property Services to address the weaknesses highlighted in the December 2018 audit report.</p> <p>New targeted checking processes have been put into operation, based on an analysis of invoice values.</p> <p>Further improvements could be made to improve controls and evidence in relation to responsive repairs. These were raised in the previous audit but still remained in July 2019. Some of these issues were due to be addressed by the new responsive repairs contract which starts on 1 February 2020.</p> <p>A number of jobs were identified that could have used National Schedule of Rates (NSR) codes to cost the work.</p> | <p>Legal advice has been sought regarding the use of sub-contractors. Discussions have also been held to resolve this matter. Following review of the contract, Legal Services have advised that current process for costing jobs using sub-contractors is consistent with the hierarchical pricing mechanisms defined within the contract.</p> <p>The new contractual arrangements are based on a simpler pricing mechanism that utilises the NSR rates to a greater extent than the existing arrangements. Although there will still be a requirement to utilise non NSR rates these will be agreed and specified in the contract.</p> <p>A detailed mobilisation plan is being developed for the new contract arrangements and will involve further instruction to staff involved in the contract management process to ensure consistency in practices. Additional contract management capacity is now in place.</p> |

| System/Area | | Audit Opinion | Areas Reviewed | Date Issued | Comments | Action Taken |
|-------------|----------------------|------------------|---|----------------|---|---|
| B | Barclaycard payments | No opinion given | <p>We reviewed purchase card expenditure from 2019/20 provided from the Procurement dashboard system.</p> <p>We used our data analytics software to provide extra insight and further information for the Council, as well as to offer suggestions for potential improvement.</p> <p>The work did not include a review of the appropriateness or application of the different processes and controls in operation at the Council.</p> | September 2020 | <p>The dashboard could be effective for providing an easy access and oversight to the expenditure on Barclaycards across the Council.</p> <p>Some transaction data is inconsistent and in areas incomplete. Some key data fields are not complete for transactions displayed on the dashboard.</p> <p>We provided extra trend and departmental information on expenditure, including areas of high and potentially inappropriate spend.</p> <p>Ongoing monitoring and analysis of spend on Barclaycard purchasing cards would allow for key trends to be identified in a timely manner. We identified some inconsistent use of Barclaycard cards.</p> | <p>A payment policy review is ongoing within in the Council. The areas highlighted in this report will be covered within the scope of this review. However, the review has been put on hold due to Covid-19, and is due to be restarted soon. The results of this review will be cascaded through the organisation, and audit will pick this up as part of the follow up process. It is planned for this work to be completed by June 2021.</p> |

AUDIT OPINIONS AND PRIORITIES FOR ACTIONS

| Audit Opinions | |
|--|---|
| <p>Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit.</p> <p>Our overall audit opinion is based on 5 grades of opinion, as set out below.</p> | |
| Opinion | Assessment of internal control |
| High Assurance | Overall, very good management of risk. An effective control environment appears to be in operation. |
| Substantial Assurance | Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified. |
| Reasonable Assurance | Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. |
| Limited Assurance | Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation. |
| No Assurance | Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse. |

| 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. |